NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN ASSESSMENT OF VULNERABILITIES FOR SHIP-BASED CONTROL SYSTEMS

by

Richard Bensing

September 2009

Thesis Advisor:	Karen Burke
Co-Advisor:	George Dinolt

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: An Assessment of Vulnerabilities for Ship-based Control Systems	**5. FUNDING NUMBERS**
6. AUTHOR(S) Richard Bensing	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Department of the Navy Chief Information Officer Presidential Towers Suite 2100 2511 Jefferson Davis Hwy, Arlington, VA 22202	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Growing asymmetric threats, such as international terrorism, have replaced the hostile nation-state as the adversary of choice. As embodied by the September 11 attacks, the United States now faces enemies that seek to create havoc and disruption in non-traditional ways. This new adversarial paradigm makes the protection of the critical infrastructure of the nation even more important than ever.

Unfortunately, this is the nation's soft underbelly. Computer-based control systems form the heart of the critical infrastructure, and these control systems are riddled with rampant vulnerabilities. A combination of industry apathy, physical challenges, and the growing reliance on the Internet by has exacerbated these vulnerabilities.

The critical infrastructure of a Navy warship is just as vital to the operation of the vessel as the national infrastructure is to the operation of the nation. Unfortunately, a ship's infrastructure is similarly permeated with control systems, which have similar weaknesses and face similar threats as their civilian counterparts.

This thesis examines the importance of the critical infrastructure on both the national and shipboard scale. Threats and vulnerabilities are established, and corrective actions are explored, with the goal of developing some strategies to improve the security of shipboard systems. As part of these corrective actions, a template security policy and a computer security checklist have been developed.

14. SUBJECT TERMS Vulnerability Assessment, Supervisory Control and Data Acquisition, SCADA, Critical Infrastructure, Information Assurance, control system	**15. NUMBER OF PAGES** 193
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN ASSESSMENT OF VULNERABILITIES FOR SHIP-BASED CONTROL SYSTEMS

Richard G. Bensing
Lieutenant Commander, United States Navy
B.S., San Diego State University, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2009

Author: Richard G. Bensing

Approved by: Karen L. Burke
Thesis Advisor

George W. Dinolt
Co-Advisor

Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Growing asymmetric threats, such as international terrorism, have replaced the hostile nation-state as the adversary of choice. As embodied by the September 11 attacks, the United States now faces enemies that seek to create havoc and disruption in non-traditional ways. This new adversarial paradigm makes the protection of the critical infrastructure of the nation even more important than ever.

Unfortunately, this is the nation's soft underbelly. Computer-based control systems form the heart of the critical infrastructure, and these control systems are riddled with rampant vulnerabilities. A combination of industry apathy, physical challenges, and the growing reliance on the Internet by has exacerbated these vulnerabilities.

The critical infrastructure of a Navy warship is just as vital to the operation of the vessel as the national infrastructure is to the operation of the nation. Unfortunately, a ship's infrastructure is similarly permeated with control systems, which have similar weaknesses and face similar threats as their civilian counterparts.

This thesis examines the importance of the critical infrastructure on both the national and shipboard scale. Threats and vulnerabilities are established, and corrective actions are explored, with the goal of developing some strategies to improve the security of shipboard systems. As part of these corrective actions, a template security policy and a computer security checklist have been developed.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF SYMBOLS, ACRONYMS, AND ABBREVIATIONS

ACD	Automatic Common Diagrams System
AGA	American Gas Association
API	American Petroleum Institute
C&A	Certification and Accreditation
CC	Common Criteria
CDS	Configuration Data Sets
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIDX	Chemical Industry Data Exchange
CIP	Critical Infrastructure Protection
COTS	Commercial-Off-the-Shelf
CPU	Computer Processing Unit
CRC	Cyclic Redundancy Check
CSI	Computer Security Institute
DCC	Damage Control Central
DCS	Distributed Control Systems
DHA	Department of Homeland Security
DIACAP	DoD Information Assurance Certification and Accreditation Process
DII	Defense Information Infrastructure
DITSCAP	DoD Information Technology Certification and Accreditation Process
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoD	Department of Defense
DoN	Department of the Navy
DoN	Department of the Navy
DoS	Denial of Service
EAL	Evaluation Assurance Levels
eMass	Enterprise Mission Assurance Support Services
FAA	Federal Aviation Agency
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FODMS	Fiber Optic Data Multiplexing System
FY	Fiscal Year
GAO	General Accounting Office
GIG	Global Information Grid
GUI	Graphical User Interface
HIDS	Host-Based Intrusion Detection System
HM&E	Hull, Mechanical, and Electrical Systems

HMI	Human Machine Interface
HSI	Human Systems Integration
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IBS	Integrated Bridge System
ICAS	Integrated Condition Assessment System
ICCP	Inter-Control Center Communications Protocol
ICS	Industrial Control Systems
IDS	Intrusion detection systems
IEC	International Electro-technical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPP	Internet Printing Protocol
IRS	Internal Revenue Service
ISA	Instrumentation, Systems, and Automation Society
ISO	International Standards Organization
IT	Information Technology
KS	Knowledge Service
LAN	Local Area Network
MCS	Machinery Control System
NERC	North American Electric Reliability Council
NIDS	Network- Based Intrusion Detection System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTAC	National Security Telecommunications Advisory Committee
OMB	Office of Management and Budget
PCCI	Presidential Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PLC	Programmable Logic Converters
PP	Protection Profile
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SECNAV	Secretary of the Navy
SLDC	Single Loop Digital Controllers
SNL	Sandia National Laboratories
SPAWAR	Space and Naval Warfare Systems Command
SPP	System Protection Profile
SSES	Ship Systems Engineering Station
SST	System Security Target
ST	Security Target
TASE.2	Tele-Control Application Service Element.2
TCP	Transfer Control Protocol
TOE	Target of Evaluation

UAV	Unmanned Aerial Vehicles
UPS	Uninterrupted Power Source
VPNs	Virtual Private Networks
WAN	Wide-Area Network
WebDAV	Web-Based Distributed Authoring and Versioning
WEP	Wireless Encryption Protocol

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to acknowledge the faculty of the Computer Science department at the Naval Postgraduate School for their understanding and patience in allowing me to complete this project in spite of the numerous personal issues that have complicated my path. In particular, I would like to express thanks to my thesis advisors, Professor Karen Burke and Professor George Dinolt, for their guidance in steering me towards this subject, which has opened my eyes to some of the hidden dangers our nation faces. Finally, I would also like to give special thanks to my daughter, Kaitlyn, who has always been, and continues to be, a source of inspiration and wonderment for me in all phases of my life.

This thesis is dedicated to the memory of my father, Richard John Bensing. His fatal illness, progressive decline, and subsequent passing, which I witnessed first-hand, was the first (but by no means the last) of the personal trials I had to endure while preparing this thesis. His pride in me lasted to the end of his days, and I have tried to remain true to his expectations. This one is for you, Dad.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS SCOPE

Supervisory Control and Data Acquisition (SCADA) systems, generically referred to as control systems, are designed to provide real-time monitoring, management, and control of a variety of different utility or industrial systems. These SCADA systems can involve hundreds or even thousands of nodes, and the sheer volume of events that are overseen requires the rendering of computer assistance to human operators. The proliferation of these systems is enormous; SCADA systems are prevalent throughout the nation's infrastructure and are used extensively throughout the Department of the Navy (DoN). They are particularly numerous at U.S. Navy ports and shore, where the management of the utility consumption of Navy vessels is an enormous, complicated, and expensive problem. The Navy also utilizes control systems to monitor and control the engineering systems, propulsion systems, and auxiliary systems on board some classes of modern warships. As technology continues to advance, and the Navy continues to search for ways to reduce its manpower base and to automate the execution of shipboard routine, this trend is likely to continue.

The purpose of this thesis is to examine the security of control systems, particularly those deployed on board U.S. Navy vessels, and to illustrate strategies to address any security weaknesses that are discovered. The scope of the analysis would include, but not necessarily be limited to, establishing the proliferation of control systems on board a ship, in order to judge the degree to which shipboard functions are impacted by this equipment; determining the organization and deployment of various control systems, in order to observe how the systems are interconnected and how the various control data could be categorized; and discovering if there is a remote monitoring capability of control systems, and analyzing the vulnerabilities of such a case. Additional security matters that would be investigated include confirming the physical security of the components of a control system network; determining if control systems were subjected to any certification and accreditation effort, verifying the degree of access to

shipboard control systems through open networks, such as the Internet or communications systems; and validating how local security policy enforces protection of shipboard control systems, and how this policy is enforced.

B. THESIS ORGANIZATION

In a general sense, this thesis is designed to illustrate why control system security is a serious issue and how security issues are addressed. Since there is significant correspondence between the significance, vulnerabilities, and security mitigations of civilian SCADA systems and Navy control systems, substantial attention is paid to both. Civilian control systems, and some aspect of their importance or some statement concerning their security, are usually used to make a base assertion. From there, the specific correlation to shipboard control systems is made.

This thesis is organized as follows:

Chapter I—Introduction—This chapter introduces SCADA systems and their importance and illustrates the organization of this work.

Chapter II—Control System Background—This chapter provides background material that illustrates the basic format and development history of control systems.

Chapter III—The Concept of Critical Infrastructure—This chapter demonstrates the criticality of control systems within the architecture of an over-arching infrastructure, as well as providing examples of their presence within both the civilian sector and the Department of Defense.

Chapter IV—Shipboard Control Systems in the U.S. Navy—This chapter extrapolates the concepts of the previous chapter and drills down to the smaller scale of a Navy warship. Specifically, the chapter illustrates the importance of Navy shipboard control systems and the likelihood of their increased implementation in the future, as well as some examples of shipboard control systems.

Chapter V—How Control Systems are at Risk—This chapter articulates the vulnerabilities of, and threats to, control systems in general, and provides some examples of attacks against control systems.

Chapter VI—Shipboard Control System Security—This chapter examines the security of shipboard systems more closely by observing weaknesses inherent in the security of all federal information systems. A high-level assessment of shipboard control system security in the Navy is also provided.

Chapter VII—Improving the Security of Control Systems—This chapter provides recommendations for improving the security of control systems. Many of the recommendations can be applied to all control systems, while one section specifically addresses shipboard control systems in particular. A template security policy, as well as a computer security checklist, were both developed for this chapter, and are represented as annexes to this thesis.

Chapter VIII—Summary and Recommendations—This chapter summarizes the conclusions reached and makes recommendations for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CONTROL SYSTEM BACKGROUND

Control systems can be generally described as collections of hardware, software, communications media, and protocols that are used to monitor and control processes, services, or commodities. The processes, services, and commodities that are managed in this way can either be at a concentrated site or dispersed to several different remote locations, and they are often critical to the functioning of our nation. These systems permeate our national economy and our industrial base, to the point that our national infrastructure is dependent upon them. Control systems are utilized in such disparate fields as utility generation and distribution, waste treatment, traffic management, industrial processing, and manufacturing. Because of this widespread proliferation, there is virtually no aspect of daily life that is not impacted in some way by these systems.

A. NOMENCLATURE OF CONTROL SYSTEMS

Since control systems are dispersed throughout so many different industries, and perform so many different functions, many different terms are used to refer to them. These terms are usually differentiated by the specific usage of the systems, the geographic area monitored by the systems, and the specific hardware used remotely in the field. The two most commonly used terms seem to be distributed control systems (DCS) and supervisory control and data acquisition systems (SCADA), although other terms are used as well.

A DCS is often characterized as a closed-loop, geographically restricted system, used at a single site, that utilizes a high-speed communications medium. A SCADA system is often described as a system that could rely on a variety of different types of communication links, and is responsible for a larger geographical area [1]. DCS seems to describe control systems that are used in manufacturing or industrial facilities, while SCADA almost exclusively refers to systems that control the distribution of utilities, such as water, electricity, and gas. However, as control systems continue to evolve, the distinction between DCS and SCADA is becoming less clear, and the names appear to be almost interchangeable.

Neither term seems to be used when describing functionally unique control systems, such as those used on board U.S. Navy warships. Interviews with members of the information technology (IT) and engineering communities in the Navy indicate that these terms are relatively unknown in those circles. Shipboard systems that encompass some aspects of utility distribution, and thus mirror the performance of common SCADA systems, are usually referred to as Hull, Mechanical, and Electrical Systems (HM&E); however, their geographic area of responsibility is small, and they incorporate additional functionality that differs from that which is traditionally associated with civilian control systems, such as participation in shipboard weapons' systems. For simplicity's sake, this thesis will generally use the generic term "control systems" to refer to any of these systems, regardless of implementation, hardware, and geographical considerations, although other terms may be used as deemed appropriate.

B. CONTROL SYSTEM COMPONENTS

A control system typically consists of a master station connected in some fashion to at least one, but usually more than one, remote terminal unit (RTU). These RTUs are in turn connected to various control equipment and sensors. The RTU receives information from the sensor elements and relays that information to the master station. The RTU can also issue directives to the control equipment to initiate an action based upon the data that the sensor delivers. These directives could either be locally determined by the RTU, or they could simply be relayed from the master station. The entire system is connected by a communications system that provides the medium for this information flow. Figure 1 depicts this concept.

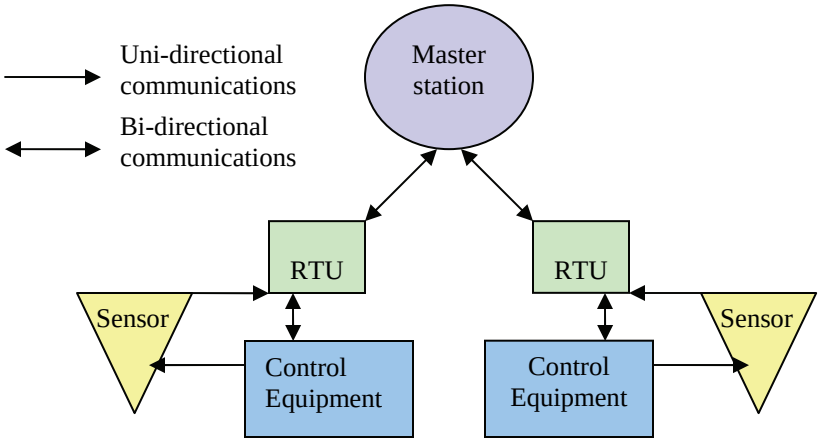

Figure 1. Simple control system.

1. Master Station

The master station is typically configured at the main site. It usually consists of a central management and monitoring station that has at least one, but perhaps more than one, human-machine interfaces (HMI) that are used to observe data as it is fed from remote sites, and for human-determined control commands to be issued to the remote sites. Master stations will collect the data that is reported by remote stations and can perform data archiving, trending, and display, as well as report generation, and may disperse these functions across several workstations. There may also be application servers present, as well as an engineering workstation that is used to perform maintenance and to configure the system. Master stations may communicate with remote stations in a variety of ways, depending upon the operating environment and the communication channels available [2].

2. Remote Terminal Units (RTUs)

Remote terminal units are deployed in remote locations away from the central site. They receive the data that is detected by the sensors and relay that information back to the master station. RTUs can also issue control commands to the control equipment in response to a certain measured condition or set of conditions, with the intent of making a corrective adjustment. RTUs can also pass information to other RTUs, either on a peer-

to-peer basis or while functioning as a relay from the master station. The complexity of the RTU varies according to the complexity of the supported infrastructure, and the logic and computational requirements are typically industry-dependent [3]. Currently, computer processing unit (CPU) advances and improvements in RTU design have given remote units the ability to directly administer control decisions, rather than receiving the command input from the master station, and remote units utilizing this capability are typically called programmable logic converters (PLCs). However, the differentiation between the two is indistinct, and these units will be referred to as "RTUs" throughout this thesis.

3. Control Equipment and Sensors

Control equipment is directly connected to the working components of the infrastructure—such as water pipes or voltage junction boxes—and manipulates them in response to directives from either the master station or the RTU. Examples of this mechanical manipulation include tripping breakers, opening and closing valves, and toggling relays [2].

Like control equipment, sensors are connected directly to the working components of the infrastructure. Sensors measure the data that is to be monitored, recorded, and, if necessary, acted upon. This data can be in either digital or analog form. Examples include fluid or air flow, hydraulic pressure, fluid level, voltage or current output, a binary state value (such as "on-line/off-line"), temperature, and vibration level.

In today's modern control systems, sensors and control devices are often coupled into a single unit. This configuration is commonly referred to as an intelligent electronic device (IED).

4. Communications System

The components of a control system utilize a variety of communication mediums to disseminate data and control information. These methods include, but are not limited to, dedicated lines, public telephone lines, microwave signals, Ethernet, 802.11, radio links, fiber optics, and satellite communications. Due to the extreme cost of

communication channels and equipment, time domain multiplexing is frequently employed to maximize the effectiveness of the least number of channels. The configuration of the communication system is dependent upon the number of RTUs, the location of the RTUs, the amount of data monitored by particular RTUs, the rate at which information must be updated throughout the system, and the availability of communications equipment, facilities, and techniques.[4] Table 1 provides more detail about the various methods of communications.

Table 1. Common communication paths (After [5]).

TYPE	DESCRIPTION
VHF/UHF Radio	VHF/UHF radio is a high-frequency electromagnetic wave transmission. Radio transmitters generate the signal, and a special antenna receives it.
Microwave Radio	Microwave radio is a high-frequency (GHz), terrestrial radio transmission and reception medium that uses parabolic dishes as antennas. The dishes are usually mounted on towers or on tops of tall buildings, since this is a line-of-sight technology.
Geosynchronous Satellites	Geosynchronous satellites use a high-frequency (GHz) radio transmission to route transmissions between sites. The satellite's orbit is synchronous with the earth's orbit so the satellite remains in the same position with respect to the earth. Satellites receive signals from and send signals to parabolic dish antennas.
Switched Lines	The dial-up network is furnished by a telephone company. This telephone line is the one that we commonly use to carry voice and data transmissions.
Private Leased Lines (PLL)	PLL is a dedicated telephone line that is a permanent connection between two or more locations that is used for analog data transmission. The line is available 24 hours a day. For the line to be used for voice communication, a voice
Digital Data Service (DDS)	DDS is a special wide-bandwidth private leased line that uses digital techniques to transfer data at higher speeds and at a lower error rate than private leased lines. The line is available 24 hours a day.

C. CONTROL SYSTEM FUNCTIONS

Because there are such a wide variety of control systems throughout the nation's infrastructure, the functionality of a particular system is dependent upon the environment in which it operates. Therefore, compiling a definitive list of functions that embraces all systems is impossible. The functions described below are typical of those found in electric utility SCADA systems, and serve as a good general example [3].

1. Data Acquisition

Information is the lifeblood of any control system. Accordingly, the collection and transmission of that data is critical to the system's successful operation. Data acquisition is the monitoring of multiple individual points of interest which, when taken collectively, allows for a "snapshot" of the state of the system at a given point in time. While this process appears to be a deceptively simple concept, it is actually composed of several coordinated sub-tasks that form the complete procedure of data acquisition. These sub-tasks include:

- Scanning the specified points of interest and storing the results within the RTU database
- Transmitting the updated information periodically to the master station
- Verification of data transmission integrity
- Conversion of the data into measurable units, as necessary
- Updating the state information

Information is usually transmitted to the master station by use of a polling scheme, whereby the RTU sends the data in response to a request from the master. This polling scheme could either be fixed-duration or round-robin. In some cases, the RTU sends the relevant data for all of the points requested by the master. However, the RTU could also send only those points whose values have changed, or whose values exceed a

specified rate of change, since the last poll request. This method, that has the benefit of reducing the processing overhead at the master station, is known as report-by-exception [3].

2. Information Display

Information display presents selected data to a human user for observation and analysis. This information is often displayed in real-time, but it can also be historical data that has been archived. The information is usually displayed in a graphical user interface (GUI) that provides a pictorial representation of the system or subsystem that is being monitored. This facilitates the observation and analysis of the data, and provides a user-friendly method to navigate the SCADA database. An example of a modern SCADA display can be seen in Figure 2.

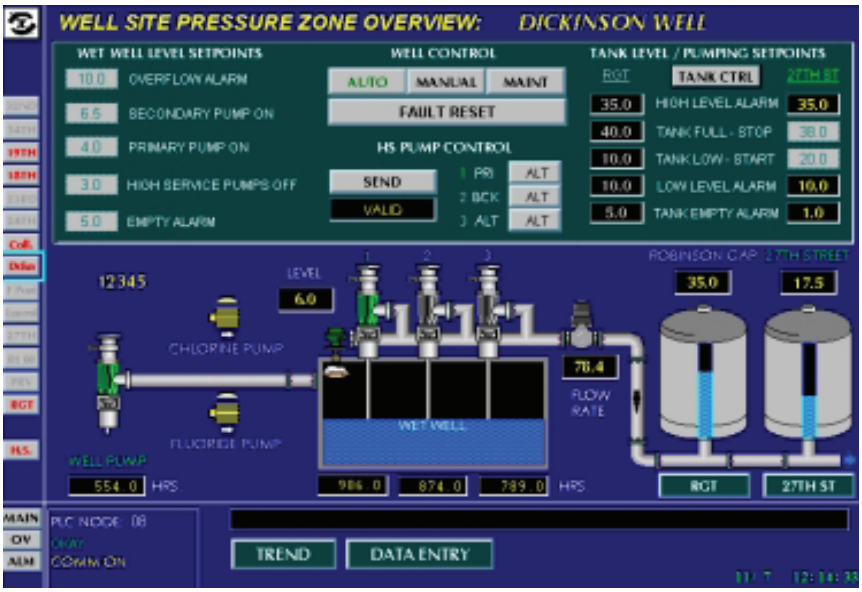

Figure 2. Sample SCADA display (From [5]).

3. Control

Control refers to the process of "actuating equipment operations at remote locations." [3] This process selects the device that is to be controlled and initiates the appropriate command to be executed, and may be done either automatically or in response to an input from a human user. Previously this control was exercised almost

exclusively by the master station, but advancements in RTU processing power and logic-handling capability has allowed many of these control commands to be executed by the RTU at the remote site. Due to the criticality of ensuring proper command execution, a check-before-operate has traditionally been performed, where the selection of the desired command is verified before execution actually takes place.

4. Alarms

Whenever an unscheduled event takes place, or a measurement is detected that is outside of accepted operating parameters, an alarm is issued. Typical components of alarm processing include identifying the sensor that detected the event or measurement, reporting the location of the occurrence, indicating the date and time of the alarm, and providing a description of the event.

5. Information Storage

Information storage is a vital process for all SCADA systems. Maintaining accurate records is necessary to ensure that government regulations are maintained and proper accounting is administered, and is also useful for planning future system operation [3]. Historical information can be used in the maintenance of system logs as well as the generation of a variety of reports. This information is also necessary for performing trend analysis, and is explained in the following section.

6. Trending

Trending is the process of collecting information about discrete events that are collected over a period of time and presenting them with a time reference. This provides a visual report that can be analyzed to glean information about the state of the system within a certain time frame. Older SCADA systems utilized oscillographic equipment to display this information, but modern systems almost universally use GUIs for this function. An example is shown in Figure 3, where the temperature readings of three different sensors, taken over one month's time, are displayed for comparative analysis.

Figure 3. Sample trend analysis display (From [6]).

7. Data Calculations

Data calculation is the manipulation of collected data in order to present it in some useful form. Single-variable calculations include the determination of averages, maximum or minimum values over given intervals, and integration with respect to time, while multiple-variable calculations include common mathematical operators such as sums, differences, products, quotients, squares, square roots, and exponentiation. Boolean operations can also be performed in order to "determine a particular state of some part of the …system not definable by only one status indication." [3]

In addition to the above functions, control systems can also incorporate more specific functionality that is dependent upon the particular infrastructure being monitored. Examples include:

- Automatic Pipeline Leak Detection
- Automatic well testing

- Water Canal Control
- Electrical Distribution Control
- Remote Pump and shutdown Controls [7]

D. HISTORY AND EVOLUTION OF SCADA ARCHITECTURE

The concept of remote control and remote indication is not a new one. Patents for these concepts were filed as early as the 1890s [3]. The roots of SCADA can be traced to the development of telemetry in the first half of the twentieth century, when advances in aircraft and rocket technology made it possible to gather information from the Earth's atmosphere and transmit it to the ground in real time, where it was used to provide accurate prediction of the weather [5]. Control systems that were utilized in industry at this time were electromechanical, and were largely used for monitoring purposes and simple indication of status. However, in the 1960s, it became apparent that there was a growing need to more effectively monitor and control the state of remote equipment, and as computer technology continued to advance, the enhanced supervisory control potential that these machines offered was recognized. Consequently, computer-based SCADA systems soon became standard throughout the nation's infrastructure.

1. First Generation

SCADA systems were initially monolithic in nature, and all processing functions were conducted via a single master system. The concept of networking was relatively unheard of, and these were predominantly closed systems with little to no access to external networks. The wide-area networks that connected the master station to the remote units were designed exclusively for communication with the RTUs in the field, and were not intended to support wider connectivity. This architecture is depicted in Figure 4.

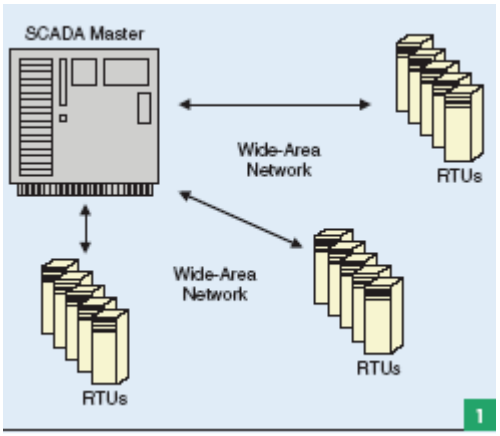

Figure 4. First-generation SCADA architecture (From [8]).

The protocols used for these communications were typically proprietary in nature, and restricted the equipment that could be used on the system. Many of them are still in use today. The protocols were often created by RTU vendors and usually were not able to communicate with the equipment from another vendor. This made it impractical for SCADA users to intermingle different types of equipment. Additionally, these protocols had extremely limited functionality, and were designed solely to fulfill the minimal requirements necessary to initiate communications with remote equipment in the field, making it impractical to introduce other forms of data traffic on the SCADA network.

Redundancy was usually accomplished by utilizing a second master station whose purpose was to monitor the primary and assume its function in case of failure. Aside from acting as a failsafe, the secondary had no other function, and its processing and computational capability went largely unused [8].

2. Second Generation

The next generation of SCADA systems saw the growth of distributed systems. Advances in local area network (LAN) technologies and equipment miniaturization allowed system functionality to be spread across multiple stations rather than concentrated into a single unit. Some stations were used to perform repeated calculations, while others served as communications stations, database servers, and

HMIs. This provided an enormous increase in processing potential, as well as a considerable enhancement of redundancy from the old primary-model. Figure 5 illustrates this concept.

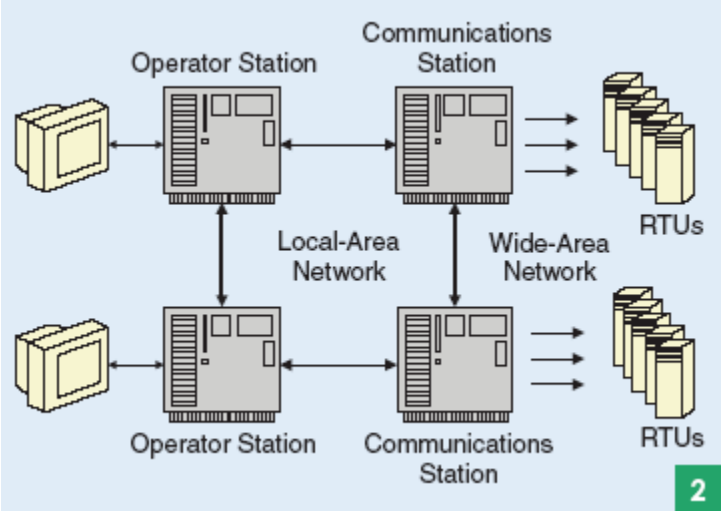

Figure 5. Second-generation SCADA architecture (From [8]).

However, this architecture still had limitations. The improved LANs had severe distance limitations, offered no enhancement for communicating with remote stations, and merely provided an easy method of connecting multiple stations at a single site. They were not suitable for facilitating long-range communications, and hence their only real benefit was enabling the clustering of multiple units at the master station. The long-range communications were still handled by the existing wide area network (WAN) technologies of the first generation, with the same proprietary and capability limitations. Additionally, the LANs themselves were also proprietary in nature, eliminating any possibility of utilizing equipment from multiple vendors on the same LAN. As was the case with the first generation, second generation systems were "limited to hardware, software, and peripheral devices that were provided, or at least selected, by the vendor." [8]

3. Third Generation

The third generation of SCADA systems, shown in Figure 6, was superficially similar to the previous generation. Distributed processing still took place; functionality

was still separated across several platforms; and RTUs still utilized proprietary protocols. However, whereas previous systems were almost entirely proprietary, third-generation systems utilized a variety of open protocols and standards.

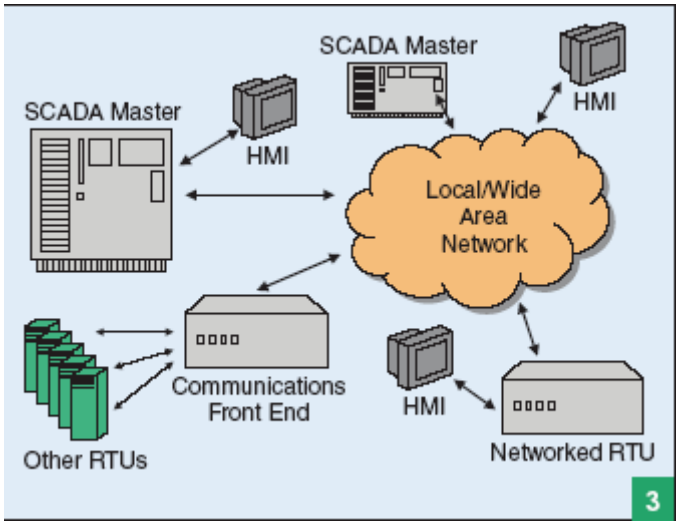

Figure 6. Third-generation SCADA architecture (From [8]).

This resulted in tremendous changes for SCADA systems. Opening the SCADA architecture in this fashion radically changed the face of SCADA, giving users the freedom to utilize almost any commercial off-the-shelf products rather than be tied to a specific vendor. With the ability to select the computing platforms and peripherals that best suited their needs, customers were able to maximize the effectiveness of their system. A side-effect of this was the elimination of SCADA vendors as hardware developers, which allowed them to "concentrate their development in an area where they can add specific value to the system—that of SCADA master station software." [8]

Another change in this generation of SCADA from previous versions—and perhaps the most significant one—was the development of modern WAN protocols such as TCP/IP. Previous SCADA systems utilized LAN protocols for distributed processing within the master station. WAN protocols incorporated this same principal, but they enabled SCADA functionality to be distributed across any part of the SCADA network. This significantly increased the "survivability" of the system, since the network could then withstand the loss of a single location and still continue to function. In addition,

WAN protocols allowed communications stations to be placed in direct proximity to remote field equipment, and offered a variety of communications media that were not available before, thereby enhancing overall communications capability at a significantly lower cost. Additional communications benefits were accrued when RTUs were equipped with network devices that connected them to a remote LAN, since this enabled direct communications with the master site.

The development of WAN technologies radically altered the landscape of the SCADA network. Robert McClanahan noted in the March/April 2003 issue of IEEE Industry and Applications Magazine that utilities might find it beneficial to develop IP-based SCADA networks and take advantage of IP-based applications that "reach beyond the utility's main campus and out into the service area." [8] This concept would have a sizable impact on the maintenance of SCADA systems, since linking remote sites with the corporate network would significantly enhance the information available to field personnel, while the utilization of IP could drastically improve voice communications between stations as well as facilitating automated and remote-control maintenance tasks such as automated meter reading. Another potential benefit is the development of a robust command and control capability, since the flow of SCADA information along an IP-based network could be remotely accessible by corporate decision-makers.

4. Modern SCADA Architecture

The continuing evolution of SCADA systems can be seen in Figure 7, which illustrates a simplified modern architecture. Supervision of the SCADA system is accomplished by the master station, referred to in the figure as the supervisory control and monitoring station. Application servers provide distributed capability and operational redundancy at the central site. System maintenance and configuration changes are accomplished at the engineering workstation, while the HMI allows human-directed monitoring, control, and analysis. Communications to remote stations, which are dispersed as required throughout the infrastructure, are handled by a variety of possible methods, including leased lines, the public switched telephone service, the Internet, or wireless devices. Remote stations handle the direct monitoring and control

capabilities in the field, utilizing SCADA-specific bus protocols to allow the RTUs and IEDs to communicate. Additional connectivity to the RTUs can be achieved via modem access, as well as through portable hand-held devices, and RTUs may have console access as well to facilitate field maintenance and diagnostic evaluation.

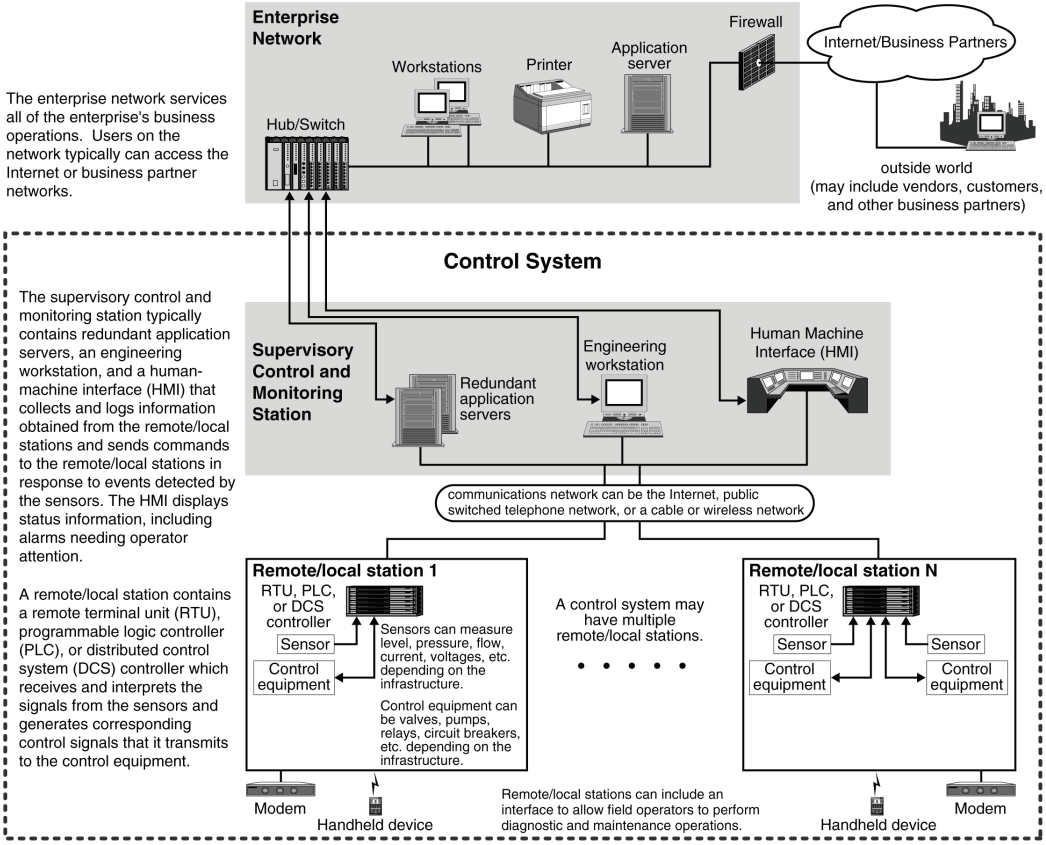

Figure 7. Modern SCADA architecture (From [1]).

E. COMMUNICATIONS PROTOCOLS

There are numerous—somewhere in the neighborhood of 200 or so—communications protocols implemented by control systems. Traditionally, legacy control systems networks were highly proprietary and hence utilized closed protocols that were specific to particular vendors. These early networks were designed for slow-speed communications that consumed a very small amount of bandwidth. Recently, control system networks began to shift away from proprietary protocols and migrate to open protocols, in the interests of increasing messaging capability. Today, general-purpose

protocols, such as TCP/IP, are used in control system networks in conjunction with open protocols and industry standards, although they possess time-delay capabilities that can introduce unwanted latency into the system.

The reason there are so many different protocols is because each control system network has different requirements, ranging from polling scheme to message size to transmission speed. The various protocols have different uses and limitations, depending on the protocol and the system. A few of these are briefly described below in Table 2.

Table 2. Some Control System Communications Protocols (After [9]).

PROTOCOL NAME	DESCRIPTION
Modbus RTU/ASCII	Most popular serial protocol in control systems. Excellent compatability with gateways. Encapsulates well with TCP/IP. Relatively unsophisticated. Slow tramission speed.
Controller Area Network (CAN)	Initially developed to connect urimary control components of automobiles. Resistant to noise interferenc. Rigorously fault-resistant.
Profibus	Most-widely accepted international standard. Can handle large amounts of data at high speed. Unsuitable for use when data transfer is small.
Foundation Fieldbus	May soon become the preffered standard of the future. Safe and flexible protocol. Often used in oil refineries and chemcal processing plants. However, proliferation is currently limited by lack of compatible devices and the slow process of standardization.
DNP3	Widely used in Europe, South America, and the United States.

Figure 7 illustrates an important difference between third-generation systems, and what this thesis considers as a “modern” system: the connectivity between the SCADA system itself and the business network of the enterprise. More companies are allowing their SCADA systems to interconnect to their corporate LAN, which can in turn lead to connection to the external Internet. As a result, once-closed SCADA systems are now more widely connected to external networks than ever before. While this practice allows system engineers to monitor the state of the system remotely, and provides important

information instantly to high-level decision-makers, it is also fraught with dangers and makes control systems vulnerable in ways they never were before [10]. This will be examined in more detail later in the thesis. Chapter III, however, will discuss why control system security is so important by illustrating the environment that control systems are most commonly utilized—that of the critical infrastructure.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE CONCEPT OF CRITICAL INFRASTRUCTURE

A. A DEFINITION OF CRITICAL INFRASTRUCTURE (CI)

One cannot truly grasp the importance of control system security without attempting to understand the notion of critical infrastructure (CI). The components of our nation's daily activities make up a patchwork tapestry, which the fabric of our daily existence depends on. The critical infrastructure consists of those components that are vital for sustaining the basic facilities, services, and installations that ensure the proper functioning of our society, such as electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking, finance, emergency and government services, and agriculture. These systems are the lifeblood of the nation's logistic, economic, and functional health and are critical for the security and prosperity of the nation. Thus, the preservation of this critical infrastructure, and the protection of the systems that control it, is vital to maintaining the nation's pattern of life.

A military unit is, in many ways, a microcosm of the nation, and is governed by the same infrastructure necessities that govern the country. Therefore, the preservation of the infrastructure of this military unit—a Navy ship, for example—is no less critical than it is for a country. The concept of CI security easily scales down from the national perspective to a ship perspective. A ship maintains its own water supply, creates its own electricity, eliminates its own waste product, and utilizes its own internal telecommunications. A ship generates its own propulsion, possesses its own emergency services, and preserves its own financial solvency. In short, a Navy warship replicates the same critical infrastructure as the nation it defends. It is therefore necessary to become aware of the importance of critical infrastructure on a national level in order to truly appreciate its importance at the shipboard level.

B. CRITICAL INFRASTRUCTURE INTERDEPENDENCE

The vast interdependence among CI components significantly complicates the problem of securing those components. None of the CI industries exists in a vacuum.

They are linked by an intricate lattice of support from one infrastructure component to the other, and any adjustment to one of these components has a profound affect on the other pieces of the puzzle.

This concept is not merely theoretical in concept. In 1998, the case of the *Galaxy 4* telecommunications satellite led to an outage of nearly 90% of all pagers nationwide, disrupted credit card purchases and automated teller machine transactions, and interfered with the communications of emergency services. Another example is electric power disruptions that occurred in California in early 2001, which affected oil and natural gas production, refinery operations, pipeline transport of gasoline and jet fuel within California and to its neighboring states, the movement of water from northern to central and southern regions of the state for crop irrigation. This led to billions of dollars of lost productivity, and stressed the entire Western power grid [11]. As these examples show, the disruption of one CI industry can have significant (and often unforeseen) impacts on others. Figure 8 illustrates just how intimately these industries are dependent upon each other.

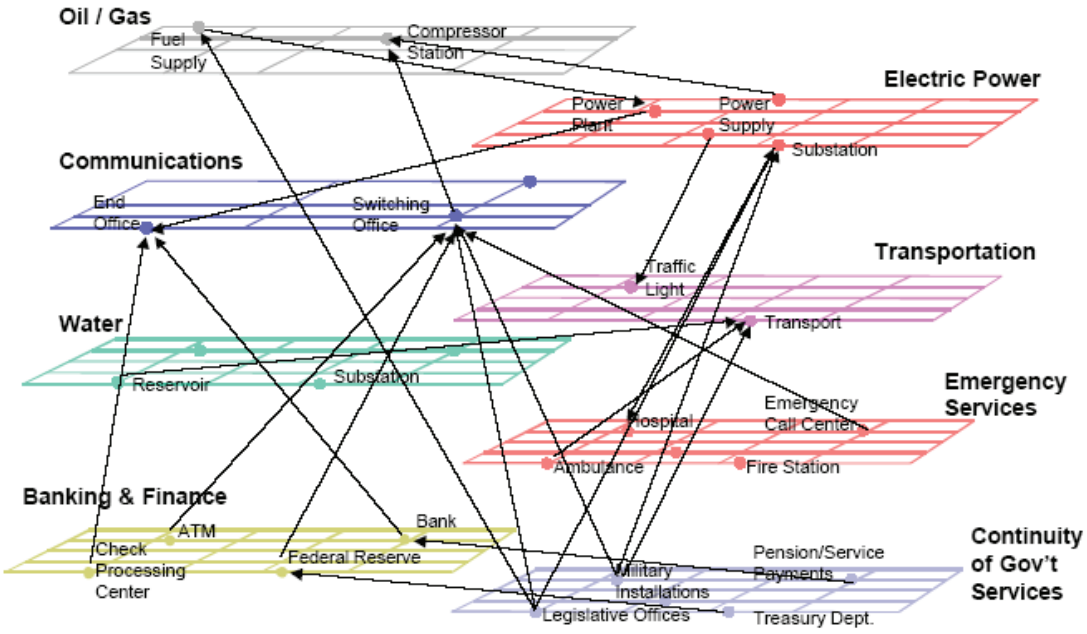

Figure 8. Critical infrastructure interdependencies (From [12]).

Critical infrastructure components have varying degrees of interdependence. Physical interdependency means that one of the components relies on the output of another in order to properly function. Cyber interdependency means that an infrastructure component depends on information that flows through some type of information medium from another infrastructure component. A third type of interdependency is geographic, when multiple infrastructure components are collocated, and changes in the environment of one component can affect all of the components in geographic proximity. Yet another type of interdependency is logical, where the state of one component depends on the state of another via a mechanism that is not a physical, cyber, or geographic connection [11]. These levels of interdependency make it difficult to predict all of the perturbations of consequences that could occur should one of the components be disrupted, because a single incident could create a ripple effect that can spread to numerous other components, as depicted in Figure 9.

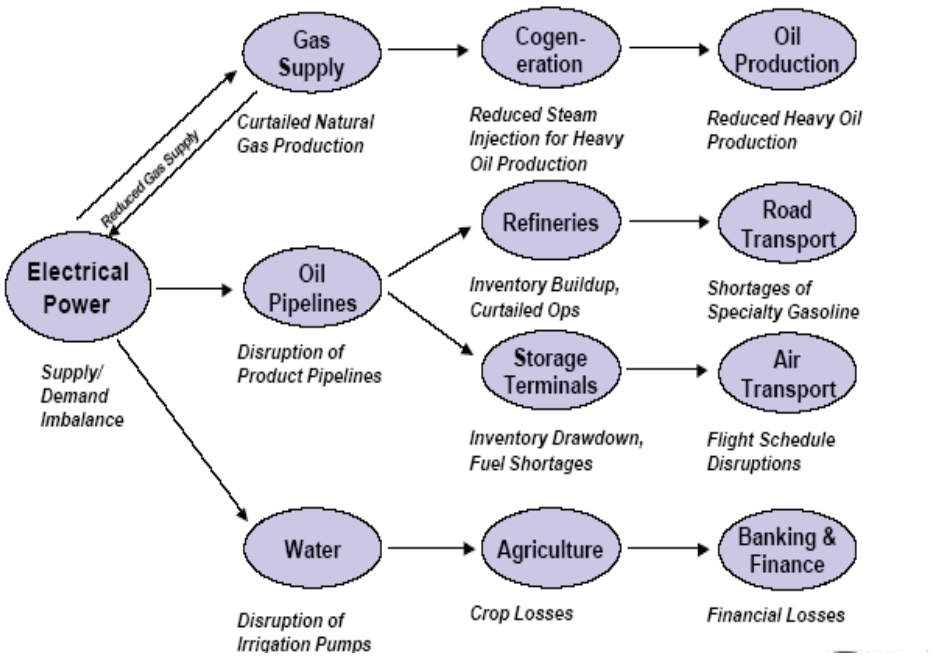

Figure 9. Cascading effect of critical infrastructure disruption (From [12]).

This lattice of interdependence is present on board a ship as well as on the national level. For example, the launching of aircraft onboard an aircraft carrier, accomplished in part by the use of catapults, that fling the aircraft from the deck. These catapults are powered by steam. A failure in the ship's internal water distribution can shut down the catapults, which in turn eliminates the ship's capability to launch aircraft, which results in a significantly degraded mission capability for the vessel.

It seems evident that critical infrastructures will become even more interconnected as information technology evolves. Identifying, understanding, and analyzing the interdependencies among infrastructures is a complex problem that shows no sign of simplification in the future. However, given the impact that these interdependencies can have on infrastructure operations in the event of some sort of catastrophic event, it is vital that this issue is addressed.

C. IMPORTANCE OF PROTECTING THE CRITICAL INFRASTRUCTURE

Because CI components are so thoroughly enmeshed with each other, and because the critical infrastructure as a whole is so vital to daily existence, the importance of protecting it has risen to unprecedented levels. The terrorist attacks on September 11, 2001, and the events that have transpired as a direct result of those attacks, have only served to bring this subject into even sharper relief.

A measure of the current importance of this topic is the degree of effort that is now being spent to specifically address it. Critical infrastructure protection has been a subject of Presidential Decision Directives, Executive Orders, and National Strategies, as well as numerous white papers, reports, and initiatives. It has spawned new government agencies whose purpose is to investigate vulnerabilities, devise appropriate solutions, and implement corrective measures. Critical infrastructure security is now a subject that is a matter of concern for countless agencies that span all facets of the government [13]. Some of this exhaustive documentation and agency involvement is described in brief below.

1. Executive Order 13010 (Critical Infrastructure Protection)

This Executive Order established the Presidential Commission on Critical Infrastructure Protection (PCCIP). It was the first national attempt to recognize the importance of critical infrastructures in the Information Age, and distinguished the threats to these infrastructures as being either physical or cyber-related.

2. Presidential Decision Directive (PDD)-63

This directive, entitled "Critical Infrastructure Protection," (CPP) was issued on May 18, 1998, and was based on the recommendations of the PCCIP. It defines critical infrastructure as physical and cyber-based systems essential to the minimum operations of the economy and government, such as telecommunications, energy, banking and finance, transportation, water systems and emergency services [14]. This directive is a call for government and civilian joint cooperation in assessing the vulnerabilities of the national infrastructure, developing strategies to combat these vulnerabilities, and implementing the necessary protections.

3. Executive Order 13228 (Office of Homeland Security)

This order was signed on October 8, 2001, and it designated an Office of Homeland Security whose purpose is to coordinate and direct the national strategy to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. This order authorizes the Office to coordinate the effort to protect the critical infrastructure of the United States against terrorist attacks. Specific industries are identified as part of the critical infrastructure, all of which typically utilize SCADA or similar control systems. This order also established the Homeland Security Council, consisting of many high-level government officials, whose purpose was to advise the President on matters pertaining to Homeland Security [15].

4. Patriot Act of 2001

Initiated in direct response to the September 11 attacks, the United States Patriot Act of 2001 was designed specifically to exhaustively define the scope of the term "terrorist," direct the security of the nation's borders from terrorists, and expand the

means of identifying, tracking, and prosecuting terrorists. The Patriot Act is divided into ten titles, each addressing a particular aspect of the struggle against terrorism. Title VII, Section 701 specifically directs increased information-sharing relating to critical infrastructure protection. Title X, Section 1016 is completely devoted to critical infrastructure protection, and was self-referred to as the "Critical Infrastructures Protection Act of 2001." This section recognizes the importance of various infrastructures in the functioning of the nation, and further illustrated the growing importance of information systems in these infrastructures [16].

5. National Strategy for Homeland Security

This document, released in July 2002 by the Office of Homeland Security, was the first national strategy aimed at specifically articulating the national effort to ensure the security of the nation from terrorism. The strategy outlines six critical mission areas relevant to homeland security, and recognizes eight major initiatives that are necessary in the protection of critical infrastructure. This document eventually led to Homeland Security Act of 2002, which established the Department of Homeland Security from the already-existing Office of Homeland Security [17].

6. National Strategy to Secure Cyberspace

This document enforces one of the eight major critical infrastructure initiatives mentioned in the *National Strategy for Homeland Security*. Released in February 2003, it is an initiative designed to unite the federal, state, and local governments, private sector, and the American people in an effort to have everyone secure the cyberspace they control, operate, or interact with. It provides a framework to organize and prioritize these efforts, with the stated goals of preventing cyber attack on our infrastructure, reducing the national vulnerability to cyber attacks, and minimizing recovery time from cyber attacks that do occur. Lead agencies responsible for specific critical infrastructures are defined. In addition, this strategy specifically discusses the interweaving of SCADA systems throughout the national infrastructure, and classifies securing SCADA systems as a national priority. One of the important precepts behind this document is the concept of a collaborative cyberspace security effort by all interested parties, such as government

agencies, private sector organizations, and individuals. This cooperative strategy is important since the costs associated with a successful cyber attack are likely to be greater than the investment in a cyber security program to prevent it, regardless of who the security investor is [18].

7. The Department of Homeland Security (DHS)

Originally formed as the Office for Homeland Security, DHS was formed by the Homeland Security Act of 2002. As authorized by this act, DHS integrates and coordinates the efforts of a broad range of government agencies in their efforts to protect the nation against terrorism. Of particular relevance to this thesis is Title II, which establishes the Office for Information Analysis and Infrastructure Protection (IAIP). IAIP merges the capability to identify and assess a broad range of intelligence information concerning threats to the homeland under one roof, issue timely warnings, and take appropriate preventive and protective action. Among its other responsibilities, the IAIP has the responsibility for critical infrastructure protection and cyber security.

8. The National Institute of Standards and Technology (NIST)

NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST has joined in collaboration with the National Security Agency (NSA) to form the National Infrastructure Protection Partnership (NIAP), whose goal is to improve the information technology security posture of the systems and supporting operations that comprise the U.S. national critical information infrastructure. An important component of this effort addresses control systems used in support of industrial operations [17].

9. The Instrumentation, Systems, and Automation Society (ISA)

ISA directly impacts the SCADA field by directing advancements in the theory, design, manufacture, and use of sensors, instruments, and computers used in measurement and control systems. It has established a standards committee called SP-99, whose purpose is to establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure

manufacturing and control systems and security practices and assessing electronic security performance [13]. This committee is concerned with control systems whose compromise (either by faulty design, human error, or deliberate cyber attack) could result in the endangerment of public safety; the loss of public confidence; the loss of proprietary or confidential information; economic loss; or a negative impact on national security.

10. Information Sharing and Analysis Centers (ISAC) Council

Presidential Unit Directive 63 recognized the need for information to flow throughout the entire infrastructure industry and called for the various infrastructure sectors to share information about threats and vulnerabilities among themselves. This requirement is fulfilled by Information Sharing and Analysis Centers (ISACs). Each ISAC provides a 24/7 operating center that monitors the health of its sector, performs analysis of incidents, and disseminates alerts and reports as necessary. In addition, each ISAC articulates impacts for its sector, enables mutual information-sharing on all threats to their particular CI sector, and facilitates cross-sector assistance during potential sector disruptions. The fourteen ISACs encompass roughly 85% of the United States' critical infrastructure, and confer among themselves regularly through the ISAC Council. The ISACs have established an excellent collaborative reputation and have jointly responded to numerous situations ranging from national-level exercises to national disasters [19].

11. Multi-State Information Sharing and Analysis Center (MS-ISAC)

The Multi-State Information Sharing and Analysis Center (MS-ISAC)—the first government entity to join the ISAC Council—is a key example of the ISAC concept. The MS-ISAC is designed to increase cyber security awareness and response at the state and local government level, acting as a central resource for gathering, and disseminating, information about critical infrastructure cyber threats. Participation is gleaned from all 50 States, the District of Columbia, local governments, and U.S. Territories. The MS-ISAC objectives include the generation of security planning analysis, the distribution of current proven security practices and recommendations, the dissemination of cyber threat early warnings, the sharing of security incident information, and the promotion of awareness of CI interdependencies [20]. The MS-ISAC is also involved in the SCADA

Procurement Project, which is a joint public and private sector effort designed to lead federal, state and local entities in the development of standardized common procurement language to encourage the integration of security into SCADA systems. MS-ISAC is significant because it is illustrates true critical infrastructure security collaboration across several different levels of government and throughout several very dissimilar industries.

The magnitude of critical infrastructure protection is self-evident in light of the spate of governmental regulation that has been written on the subject over the last decade. The government clearly sees the importance of protecting itself from the potentially disastrous consequences of a disruption in these basic services and commodities. As much of the above documentation suggests, protecting the critical infrastructure from the cyber threat is a major facet of an effective security effort.

D. CONTROL SYSTEMS IN THE CRITICAL INFRASTRUCTURE

The components of our nation's infrastructure require a considerable degree of automation, monitoring, and control. Many of these components are tremendously vast and complex, and the volume of data to be collected and the number of decisions to be made is beyond the capability of human assimilation. Other components are simply too critical, or require too much precision, to allow for human error. In all of these instances, it is necessary to introduce the computer into the control systems environment in order to provide this depth of monitoring and control.

1. Civilian Sector

Control systems are intricately interwoven into numerous ordinary activities and services that are so common-place that we typically take them for granted. SCADA-controlled activities stretch across a wide range of subjects and which are critical to the function of our nation. The magnitude of their influence is so great that any attempt to categorically illustrate their prevalence is almost ridiculous and is, beyond a few words of description, patently unnecessary. Control systems provide monitoring and control of utility services such as oil and natural gas pipelines, water treatment and distribution, wind power, and electric power generation. Additionally, they are used heavily in public highway transportation systems as well as mass rapid transit. They are also vital to

chemical production and processing, nuclear facilities, and modern manufacturing and industrial sites [13]. Virtually no aspect of daily life is untouched by their presence. Therefore, one cannot secure the critical infrastructure without also securing the control systems that manipulate the infrastructure.

2. Department of Defense (DoD)

Control systems are just as prevalent in the DoD as they are in the private sector. The armed forces are an enormous sub-section of our society divided into many smaller units that are spread throughout the world in a variety of environments. Each of these environments has the same requirements as any other population center in civilian life—sanitization, electrical power, communication networks, and mechanization of industry. The examples below are provided to demonstrate the depth that control systems have penetrated military critical infrastructures.

a. United States Air Force

(1) In 1996, Black & Veatch Special Project Corporation, Overland Park, Kansas, was awarded a $6,478,022 contract for the complete design and construction of the water storage and distribution CONTROL system on Kirtland Air Force Base in New Mexico [21].

(2) The electrical service and distribution facilities at Edwards Air Force Base are monitored by a control system that was installed in 1990. This system controls "motorized circuit switching for automatic remote switching of the circuits and loop feeds, as well as recording consumption and demand readings [22].

b. United States Army

(1) In 2003, AQUIS modeling software was incorporated with the existing water distribution system used at Fort Drum, Washington. This provides improved capability to "monitor the distribution system at all times, detect problems or changes in operation, model and simulate solutions to problems, improve water system performance and efficiency, compute travel times of simulated contaminants, and predict future distribution system operation." [23]

(2) After numerous violations in its wastewater treatment facility, Fort Bragg installed a new control system to monitor 26 remote sites. This improved system eliminates the need to have a full-time human observer at each remote location and provides remote site control for all remote sites, generating an estimated sixty percent labor reduction [24].

(3) SCADAWare designed control systems for deployable power plants and delivered these products to the Army and the Air Force. These systems have been utilized in Afghanistan, Iraq, and Qatar [25].

c. United States Marine Corps

(1) In the face of a growing need to reduce electrical power consumption despite a rising demand in load requirements, Pacific Northwest Laboratory installed Decision Support for Operations and Maintenance (DSOM) control systems at the Marine Ground Combat Center at Twentynine Palms in 1994 and at the Marine Corps Recruit Depot at Parris Island in 2000. Since these installations occurred, Twentynine Palms has had no critical outages, and Parris Island is becoming one of the most energy-efficient military installations in the country [26].

(2) Following this installation, new control systems were installed for the Parris Island wastewater management plant and the remote Weapons Area Steam Plant. Upon the completion of this installation, a third project was implemented for energy-intensive buildings at the Depot [27].

d. United States Navy

(1) The U.S. Navy Trident Submarine Base at Kings Bay, Georgia, utilizes three different control systems for electrical power distribution. One system integrates the purchased power from the local utility company with the master control module of the station, while the two other systems control the Submarine Base Traffic Control and Water Utility Distribution [28].

(2) The Naval Surface Warfare Center utilized over fifty years of process control experience by upgrading the burner and management control system at the Naval Air Engineering Station in Lakehurst, NJ. The resulting combination of PC-software-based SCADA, single-loop digital controllers (SLDCs), and relay-ladder logic burner management components has resulted in a safer system, increased operator comprehension of the processes they are controlling, and enhanced data acquisition [29].

(3) The Naval Public Works Center in San Diego incorporated a web-based profiling software interface with its existing electrical distribution control system, allowing users to view energy consumption and to highlight potential problems [30].

Clearly, a military unit possesses the same types of critical infrastructure as a nation, and both types of infrastructure are heavily dependent upon computerized control systems. The growing interest in protecting national CI security should be mirrored by a similar interest in protecting military critical infrastructures, and implications about the security of national control systems are just as applicable to the military control systems.

Understanding the value the government places on protecting the nation's critical infrastructure, and appreciating the degree to which control systems have infiltrated so many facets of our existence, is necessary to truly grasp the seriousness of the control systems security problem. The proper functioning of our country is intimately dependent upon the health of the critical infrastructure, and protecting this infrastructure is of paramount concern. On a smaller scale, the proper functioning of a military unit, such as a naval vessel, is equally dependent upon the protection of its own critical infrastructure. Chapter IV will demonstrate that the critical infrastructure of a ship is analogous to the critical infrastructure of a nation, and that importance of secure control systems is just as vital.

IV. SHIPBOARD CONTROL SYSTEMS IN THE U.S. NAVY

Much of the discussion to this point has focused on the security of control systems in a general sense. The purpose of this was to place the idea of shipboard control systems in the proper context, in order to clearly define the relevance of their security. The importance of control systems has been established, their vulnerabilities have been demonstrated, and a framework that describes the current direction of mitigating those weaknesses has been articulated. Although they may operate behind the scenes and beyond our everyday thought, control systems are a vital and integral part of our daily lives, and the security of these significantly vulnerable systems is crucial to maintaining the daily rhythm of the nation. These broad principles can in turn be applied on a lesser scale to the environment of a U.S. Navy warship.

A. IMPORTANCE OF SECURING SHIPBOARD CONTROL SYSTEMS

Protecting the critical infrastructure is vitally necessary in order to ensure that the daily processes of the country continue to function, but the protection of the critical infrastructure of the Navy is no less important. The National Security Agency's simulated exploitation of the national electric grid in 1997 not only demonstrated the vulnerabilities of U.S. Navy command-and-control systems, it showed how the disruption of SCADA systems could impact military capability at the strategic and operational level. Disruption of control systems, specifically shipboard control systems, could also impact military capability at the tactical level as well.

U.S. Navy warships are mobile and self-contained battle vehicles with extraordinarily sophisticated offensive weaponry, but many of the vital systems on board these vessels—such as electrical routing and shipboard propulsion—are governed by control systems. Therefore, the protection of these systems is an important consideration in preserving the military capabilities of these vessels. This importance is likely to become even more profound when viewed in light of the Navy's current approach to using computer-based technology to enhance the conduct of shipboard operations.

1. The Navy's Evolving Mission Focus

The United States Navy has been undergoing a metamorphosis for the last fifteen years into a sleeker, more efficient fighting force. The cost for maintaining a defense structure that is configured to meet an outdated adversarial model is a luxury that cannot be afforded. Several rounds of base closures have eliminated dozens of Navy facilities throughout the world, while a fleet that once possessed almost 600 ships in the mid-1980s has since been reduced to less than 300. Repeated reductions in manpower over this time, seeking to eliminate unnecessary duplication of effort, have left the Navy at its current level of roughly 364,000 active duty personnel.

Despite these changes, there has been little, if any, lessening of the importance placed upon the Navy for national defense. In addition to traditional tasks such as maritime dominance and sea control, the Navy is now tasked with new requirements as a result of the Global War on Terror. This concept is embodied by "Sea Power 21," the documented vision of Admiral Vern Clark designed to provide top-level guidance as the Navy evolves from its traditional maritime force structure to one which is more readily incorporated into a joint, flexible, and global military capability.

In order to seamlessly integrate into a fused national military environment, the Navy has decided to "reduce overhead, streamline processes, substitute technology for manpower, and create incentives for positive change," and to eliminate non-essential legacy systems and platforms in order to achieve enhanced war-fighting effectiveness in the most cost-effective manner [31]. Thus, the mantra throughout this transformation is "do more with less." This goal of obtaining maximum effectiveness is demonstrated in the Navy's utilization of technology to design destroyers, cruisers, and littoral combat ships that significantly reduce crew manpower requirements of current Navy vessels [32]. Clearly, the Navy is attempting to build a force that can increase its combat capabilities while maximizing its available manpower and resources. An obvious means of achieving this end is automation.

2. The Trend towards Automation

Technology is considered a force multiplier, so that the combat power of the available fleet is, because of its sophistication, far in advance of what would normally be expected of a conventional fleet of comparative size, and this concept plays a key role in Admiral Clark's vision. According to the General Accounting Office (GAO), the vast majority of the total costs of a ship—about 65 percent—consist of operating and support costs incurred over the lifetime of the ship, and roughly half of these operating and support costs is due to personnel costs. In order to reduce these costs, while maintaining operational effectiveness, the Navy is implementing what it calls Human Systems Integration (HSI) in order to more perfectly categorize which tasks must be performed directly by Navy personnel and which can be delegated to machinery, resulting in the "minimization of personnel requirements while maximizing gains from technological applications."[32]

By automating the management of whatever utility or service they control and minimizing the number of human operators, SCADA systems in the critical infrastructure industries perform precisely this function. Ship-based control systems can perform this same task on a smaller scale. Therefore, it seems obvious that the utilization of control systems will be an important part of any attempt to automate shipboard operations. As control systems become more involved in the execution of a ship's operations, the importance of protecting these systems becomes more acute.

3. Remote-control Capability in the DoD

Remote-control capability within the Department of Defense has already become a fact of life, and this capability is likely to become more commonplace as technology advances. The use of armed unmanned aerial vehicles (UAV) in the Middle East (such as the Predator and its more capable cousin, the Reaper) for remote-controlled airborne reconnaissance and ground support attack missions is expected to increase as U.S. troop reductions in the Middle east begins [33]. Another remote-control example is the unarmed Global Hawk UAV for remote-control surveillance and intelligence collection, which is used extensively to supplement the activities of manned reconnaissance aircraft

such as the Air Force RC-135 and the Navy EP-3E. Not only are sophisticated unmanned surveillance platforms seeing more and more use, but their utility is now appreciated by an ever-growing audience, since ground combat troops are now able to view high-quality surveillance images that previously were available only for higher-echelon commanders thanks to the distribution of hand-held devices called Rovers [33]. Clearly, remote control is a developing trend within the DoD.

The Navy does not utilize UAVs as extensively as the Army and Air Force, and has no plans to operate them as combat aircraft from aircraft carriers, but the development of the Navy Fire Scout unmanned helicopter indicates that it is still a participant in the remote control trend. However, automation within the Navy will almost certainly be centered on control systems and their manipulation of the critical infrastructure of Navy warships. This capability is partially embodied by *U.S.S. Paul F. Foster* (DD 964).

The *Foster* is a decommissioned Spruance-class destroyer that was designated as the Navy's Self-Defense Test Ship in March 2003. This ship's mission is to provide the Navy with information about self-defense systems by participating in live-fire exercises and using its defense systems to in response to attacks. During these exercises, the ship is unmanned in order to provide a testing environment that provides no danger to personnel, and shipboard navigation and weapons control are done remotely from shore. While this capability is not standard throughout the fleet, it is not hard to imagine this concept being examined for possible operational employment. The advantages enjoyed by the UAVs, the paradigm of current Navy ship design, the Sea Power 21 vision to minimize manpower and maximize effectiveness, and the operational direction of the Navy's current mission all seem to make this an almost certain development in near future.

Even if the remote-control concept does not develop, it seems certain that the Navy will carefully examine the practicality of conducting shore-based monitoring and control of vital systems, in the interests of further reducing shipboard manpower requirements. Shipboard mission areas that are not critical to the actual operation of the ship are already candidates for this type of remote capability. For example, the Navy has been investigating the feasibility of conducting cryptologic intelligence collection by

shore-based personnel utilizing ship-installed sensors and equipment, thereby reducing or eliminating the presence of permanent cryptologic personnel on board ship. In light of this, it seems evident that providing critical ship's systems some measure of remote-control capability is destined to become reality.

Utilization of control systems within a ship's critical infrastructure is an inevitable consequence of technological advancement and an altered mission focus by the Navy. There are an extraordinary number of activities on board a ship, such as calendar-based maintenance, that need to be conducted on a regular basis that are manpower-intensive and repetitive in nature, and while these activities may be curtailed for the duration of an exercise on the *Foster*, they cannot be ignored for longer periods of time. Other evolutions, such as emergency response or underway replenishment, require precise harmonization among different watch sections of the ship in order to achieve the desired outcome. Any serious attempt to cut shipboard manpower of operational vessels must address the efficiency and effectiveness of these activities. Likewise, any attempt to operationally utilize remote-control vessels requires the implementation of some means of constantly monitoring and controlling navigation, propulsion, engineering, and weapons systems. Both these conditions would necessitate extensive use of shipboard control systems on the ship. The inclusion of control systems within the ship's critical infrastructure necessitates that proper attention is paid to the security of these systems, some of which will be discussed in the following sections.

B. NAVAL SHIPBOARD CONTROL SYSTEMS IN BRIEF

The Navy has had some form of control systems on its vessels for many years. The very nature of a warship, which must be able to respond to many different types of casualty situations with no expectation of outside assistance, demands some means of monitoring the status of vital equipment and of quickly exerting control in order to maintain maximum combat capability. The status of the different parts of the ship is constantly monitored from a few centralized watch stations. Should a casualty event occur, such as flooding or a fire, there are actions that can be keyed from these watch stations—for example, the release of fire-fighting agents, or the securing of electrical

power—that can either prevent further damage to the ship or eliminate the dangerous situation itself. This activity mimics, in a crude way, the operation of a SCADA system.

Navy shipboard control systems differ considerably from SCADA systems found in regular utility and industrial applications. One of the characteristics of regular SCADA systems is that they usually follow the basic architecture described in Chapter II, where at least one, and possibly several, master stations receive input from, and issue control commands to, remote elements, generally dispersed across a large geographical area. Another characteristic is that they are designed to produce a particular service or commodity, such as electrical power to a city, and distribute it under carefully designed conditions. These services and commodities are so large and complex that the SCADA systems that control them are generally specialized for that particular function.

Yet a third characteristic is that, while there are generally specific vendors for various parts of the SCADA architecture (RTUs, sensors and actuators, and software applications, for example), there is usually unity within the broad subdivisions of the SCADA system. For example, the analysis and monitoring software is generally the same, regardless of the specific computer terminal it is run on. Similarly, RTUs are often from the same manufacturer, and HMI stations themselves are many times hosted on the same operating system. This unity within these subdivisions is breaking down as the industry is trending towards components that are interoperable, but it is not quite the norm yet, and in cases such as the software applications that house the monitoring, control, and analysis software, it may never occur.

Control system networks on naval warships, however, do not share these characteristics. Shipboard systems monitor a considerably smaller geographical area, and because of this, it is tempting to suggest that they are less complex than their civilian counterparts. However, a ship parallels the functionality of a floating city, as has been mentioned previously, and so it possesses utility functions—electrical power generation, conditioned air distribution, fuel dissemination, and water treatment facilities—that would be expected in a city. Additionally, naval vessels also have other concerns that are not found in a city, such as monitoring and control of propulsion systems and the routing of firefighting agents. Thus, whereas a normal SCADA system only needs to handle one

particular category of service, a shipboard control system must often need to be able to accommodate several. In addition, the Navy will utilize several different systems to perform these tasks, often in such a way that it appears as if functionality is duplicated by these disparate systems, and this differs markedly from the trend discussed in civilian SCADA systems. Perhaps because of this, there does not seem to be a strict master-substation relationship anywhere within the various convolutions of the Navy control system, at least not to the level of rigidity that is found in normal SCADA systems. Yet despite these differences, the Navy does utilize control systems that mimic the function, if not the form, of civilian SCADA systems, and these systems will be discussed in the following section.

C. HULL, MECHANICAL, AND ELECTRICAL (HM&E) SYSTEMS

The combination of shipboard systems that is conceptually most comparable to industrial SCADA systems are defined in general as Hull, Mechanical & Electrical (HM&E) systems. These systems, and their associated networks, are designed to support event-based or interactive-based machinery control and information with established real time constraints of propulsion, auxiliary and other mission critical and mission essential ship system equipment. An HM&E system collects data from a variety of sources throughout the ship and is used to constantly evaluate the health of ship systems. The information that is monitored and distributed includes data from the engines and electric plant, as well as shipboard machinery data. Information is typically collected in real-time context, but can often be generated from historical sources as well, and is usually supported by some method of visualization aid which is often graphical in nature.

Computerized control systems have, in large part, been born as part of a shift in the way the Navy conducts the maintenance of its equipment. Until the mid-twentieth century machinery was run until it literally failed to function, at which point it was simply repaired or replaced. This method of maintenance is accurately known as run-to-failure. Since World War II, as machinery became more complicated, the Navy began conducting preventative maintenance, which was periodic maintenance performed at regular intervals in the hopes that this would stretch the operational service life of the

equipment by effectively restoring it to a state commensurate with an earlier point in time. This method has given way to a new means of maintenance known as condition-based maintenance. This means that structural characteristics and vibration patterns pf machinery can be analyzed, compared against known parameters, and a probable degradation can be detected and responded to prior to actual system failure [34]. Because of this level of sensitivity, the employment of control systems on board ships can often serve the purpose of predicative maintenance just as much as automatic system manipulation.

Research for this thesis uncovered many different shipboard systems that perform some type of function that is analogous to those that are performed by a typical SCADA system. These systems often perform different functions, have varying levels of proliferation, and exert different levels of control upon their monitored systems; however, some of the functionality of particular systems appears to be duplicated by other systems, and many of these systems actually act in concert to conduct the coordinated HM&E effort. There is a fairly bewildering variety of configurations that are installed on Navy ships, with variations existing that could be dependent on ship class, or even on individual ships themselves. Some of these systems will be discussed briefly in the following sections.

1. Machinery Control System (MCS)

The Machinery Control System (MCS) is designed to provide centralized remote monitoring and remote control of propulsion, auxiliary, fuel, fuel fill and transfer, damage control, and ballast systems. Since equipment and system configuration can often be ship-specific, or at least class-specific, “MCS” appears to be a generic term that is used to describe the consolidation of interior ship circuits and equipment that are associated with basic ship alarms, monitoring and control systems, and specific software/hardware applications. Functionality of the MCS seems to vary depending on the vessel it is deployed on.

MCS used to be an older console-driven system that made use of electromechanical displays and indicators, but this trend has been replaced by a networked PC open architecture that provides graphical representation of monitored systems. HMI stations utilizing the Windows operating system (apparently either XP or 2000) are typically provided to provide monitoring and control of selected ship's systems, while data servers are usually used for storage of historical data. Information flow between the MCS and its components and associated applications takes place along an Ethernet LAN which is typically fiber-optic, and which is commonly referred to as Fiber Optic Data Multiplexing System (FODMS). On the *Arleigh Burke* class destroyers, the fiber optic network interconnects the above-mentioned systems with Aegis combat systems.

The MCS interface is a graphical representation of the system, or sub-system being operated, providing the operator visual reinforcement of the operation of the basic system and the functionality of subsystem components [35]. This type of graphical user interface provides a rapid training transition from older interfaces and is much more intuitive for the user. The display can present the operator with monitoring data, control interfaces for equipment operation, or both. This type of interface is fairly common for this modern breed of shipboard control systems.

There is no standard description for MCS because the configuration is not consistent throughout the fleet, but some of the basic alarms and systems it encompasses are as follows:

- Standard Ship Alarm System, which includes many of the ship's auxiliary systems. Depending upon the ship type, these systems include the bilge alarm system, ship's draft alarm system, emergency eyewash system, ordinance intrusion alarm system, various firefighting activity status systems, and several chilled water and chilled air systems.

- List Control System, which allows for the draining and filling of ballast tanks to compensate for the ship's list.

- Fuel Control System, which controls and monitors the pumps, valves, and storage tanks that make up a ship's fuel dispersal system. For aviation-capable ships, this includes JP-5 fuel.

- Damage Control System, which is the subsection of MCS that deals with monitoring and controlling the ship's effort to recover from damage resulting from combat, fires, breached hull, and flooding.

In addition to these aforementioned systems, the MCS also interfaces with other control systems, such as the Integrated Condition Assessment System (ICAS), the Automatic Common Diagrams System (ACD), and the Integrated Bridge System (IBS). MCS gathers information from these, and other, systems to manipulate the control systems that effect changes in ship's machinery.

2. Automated Common Diagrams (ACD)

ACD was developed as a result of a line of programs aimed at improving the damage control capabilities of Arleigh Burke destroyers. This process began simply by creating a set of tabbed "common diagrams" of system schematics that outlined all critical systems of a ship, identified interfaces, and described dependencies so that decision-makers would immediately know the impact of isolating one system and restoring another. While this was useful, these hard-copy diagrams were voluminous and the process of selecting the correct diagram was laborious and time-consuming. The natural solution to this was to present these diagrams across a computer network, and this led to the birth of ACD. The system incorporated several merging technologies and developed into the product that is in use today. Although its functionality strays beyond the bounds of HM&E (since it has connectivity to combat systems as well), it may still be considered as an HM&E system.

ACD is designed to provide standardized damage control information throughout all necessary spaces in the ship in order to coordinate the vessel's effort to recover from damage incurred from battle damage, fires, and flooding. The system carries out several specific functions in order to fulfill this overarching directive. The first function is to provide detailed diagrams of the ship's piping, ventilation, and electrical systems.

Examination of these diagrams can allow personnel to determine exactly where steps can be taken to prevent the escalation of a casualty event (for example, which electrical systems to secure in the event of a flood, or which ventilation systems to shut down to prevent the spread of a fire). This allows for the event to be isolated and combated as quickly as possible. Another function of ACD is to provide a variety of consistently updated status reports on all monitored equipment and spaces. These status reports include HM&E equipment such as propulsion, chilled water, and electrical power distribution; combat systems such as the SPY radar; and damage control information such as status level of the fireman and readiness level of damage control repair stations. Updates to these status reports are provided via manual insertion by a human operator or by signals received from the MCS. The third function of ACD is to allow for control of selective systems and equipment via the MCS interface. Operators at the ACD workstation that is the designated Station in Control can initiate a control request to the MCS, which will then automatically perform the desired mechanical manipulation. Systems that can be controlled in this fashion include manipulation of remote-control valves on the fire main and the emergency wash-down countermeasure system. Propulsion, electrical, and auxiliary equipment is probably controlled in the same manner [34]. Work has been done to allow ACD to exercise direct control over chilled water return and flow, but it is not known whether this capability has been incorporated in the fleet.

ACD consists of a collection of UNIX-based damage control workstations that comprise a damage control network. Each of these workstations has the ACD program loaded and they are capable of sharing information on a peer-to-peer basis. FODMS provides the medium for this information transfer. The workstations are located in Damage Control Central (DCC), which is the central hub of the ship's damage control effort; key command and control spaces such as the bridge and the Combat Information Center; and the Damage Control Repair Stations. The system has been demonstrated to be portable to Windows and Linux operating systems as well. ACD information is presented in a graphical user interface that allows the user to get a pictorial representation of the status of ship's systems and soft-copy replications of the ship's diagrams.

3. Integrated Condition Assessment System (ICAS)

ICAS is the Navy's Program of Record (POR) for automated machinery condition monitoring and assessment, and is installed on 14 different classes of ships and 97 different individual vessels. Developed by the IDAX Corporation, it is a Windows-based predictive maintenance program that combines performance-monitoring techniques with computerized maintenance management. ICAS displays machines, systems, and sensors via graphical diagrams, and is able to monitor and predict machinery failure by comparing sensor data from a variety of sources to established performance criteria. In addition, it automatically logs performance data, stores it for future evaluations in a database folder, and alerts the operator with a visual or audible message whenever a material condition beyond allowable tolerances is detected [36].

ICAS performs several functions. First and foremost, it is a detailed monitoring tool, gathering input on a number of critical ship systems in order to constantly evaluate their health and status. Depending on the input mechanism, these inputs are sampled several times a minute in order to provide real-time information with a high degree of accuracy. This information is presented to human users via a graphical user interface on an ICAS workstation, which presents a pictorial representation of the system being monitored as well as the empirical results of that monitoring. The range of systems that ICAS monitors can include main propulsion, controllable pitch propeller, ship service gas turbine generator, air conditioning, refrigeration, fuel oil service, main propulsion lube oil, fire main, seawater pumps, and pressurized air. Figure 10 depicts one example of this graphical display.

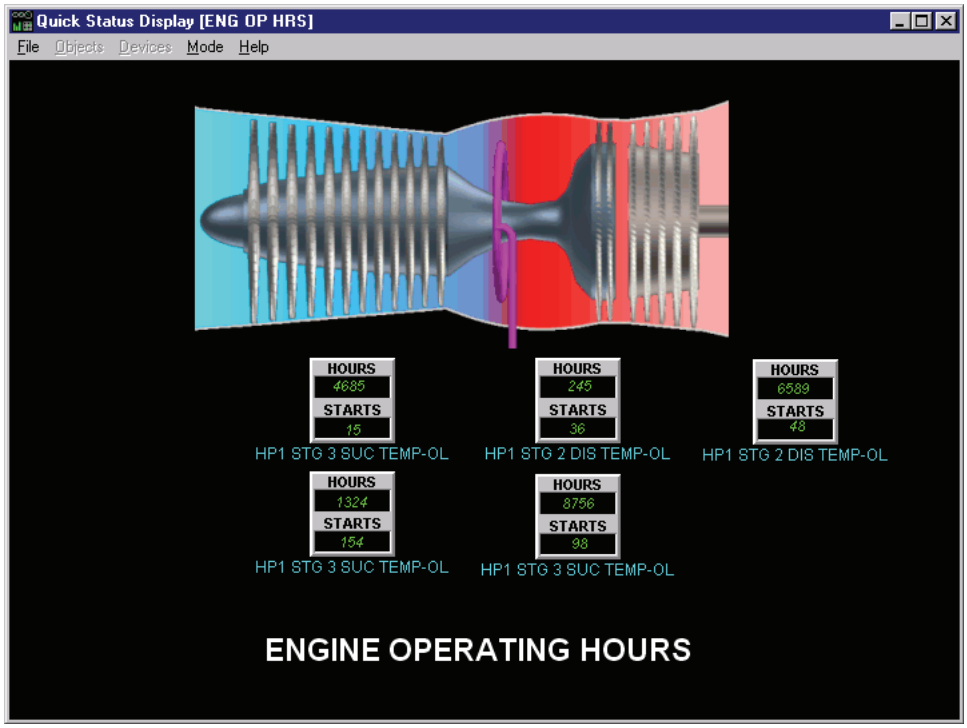

Figure 10. Gas Turbine Engine Status Display (From [37]).

In addition to this monitoring function, ICAS can also alert the user whenever a measured value is not within a specified tolerance. Whenever such an alarm state occurs, ICAS will gather information about the associated state and display it to the user, allowing maintenance personnel to not only quickly isolate the possible fault but to perform validation actions. This rather simple diagnostic capability is enhanced by the systems capability to combine several different inputs and utilize logic rules defined within the particular ICAS configuration to determine situations requiring maintenance. ICAS also serves as a troubleshooting tool, maintaining links to Navy maintenance publications and scanning these publications whenever a faulty condition occurs; should this search discover maintenance procedures that match the measured conditions of the fault the user will be provided a link to the appropriate maintenance publication.

Yet another function of ICAS is to provide for extensive fault analysis, by allowing users to define events which, when triggered, write data to the disk at an enormous accelerated rate and which can later be studied in order to determine the cause of equipment failure. ICAS also serves as a computerized maintenance log,

automatically entering received inputs into a pre-designed log sheet and eliminating the need for hand-written logbooks. Finally, ICAS can be used to perform trend analysis on data stored within its database over time, allowing personnel to detect degradation of equipment in advance and perform repair or removal prior to actual system failure.

ICAS usually consists of four to five 5 HMI computers, each installed in one of the major machinery rooms on board a ship, all connected in some fashion by an ICAS LAN. The method of interconnection varies depending upon the ship class and, presumably, individual vessels. On many operational warships, this is a hardwired LAN; however, the Navy's Self-Defense Test Ship is utilizing wireless technology and it seems likely that this method has been deployed throughout the active fleet to some degree. HMI computers are referred to as workstations if they are enabled for direct monitoring and analysis of data, and these machines are connected in a peer-to-peer configuration that allows for information sharing among the workstations. HMI computers known as clients may also be used simply to view data that other stations are gathering, or to gather information from a data store, but these computers are not directly connected to any machinery and do not perform any data processing or acquisition of data.

Each ICAS workstation has a particular area of responsibility where it monitors its assigned machinery and stores that information locally in a Borland Database Engine 5.1. Workstations are customized according to the particular ship they are installed on, and the particular space they are monitoring, by the application of Configuration Data Sets (CDS) that define the environment the ICAS operates in, determines what algorithms will be used in processing data, and what measures will be taken in processing the data that is collected. The flexibility of CDS means that ICAS is a highly adaptable monitoring tool that can be used for a wide variety of inputs in a wide range of environments.

Research has revealed contradictory data regarding information flow in ICAS. Interviews with NAVSEA personnel indicate that ICAS only monitors machines and equipment, and does not exert any control over those systems. However, ICAS is installed with connections to external PLCs, which are used in SCADA systems to direct the movement of control equipment that performs actual manipulation of field devices; it

seems unlikely that ICAS would allow connection to such devices unless it were capable of exerting some form of control over the monitored systems. The ICAS operator's manual does not explicitly discuss control signals in depth; however, it clearly defines a control output as "the predefined action ICAS takes when sensors reach certain parameters." [37] Additionally, the manual explicitly states that control outputs can only be initiated by ICAS itself, and cannot be instigated manually by a user through the HMI. Additionally, ICAS interfaces with the MCS, which definitely does possess control capability. These facts seem to indicate that ICAS does probably perform both monitoring and control of systems, although it is not clear if it merely passes along control signals from the MCS or if, as seems most likely, it generates and disseminates those control signals itself.

Following the dictates of "Sea Power 21" and mirroring examples throughout the rest of the DoD, Navy shipboard control systems are becoming more involved in ship operations than ever before, just as civilian control systems are becoming more integrated into the nation's critical infrastructure. In both instances, the incorporation of computer-based technology has made these operations more productive and less manpower-intensive. But is there a price to be paid for this efficiency? Chapter V will answer this question by examining the threats to, and vulnerabilities of, the critical infrastructure and its control systems on a national scale.

THIS PAGE INTENTIONALLY LEFT BLANK

V. HOW CONTROL SYSTEMS ARE AT RISK

The previous two sections demonstrated how pervasively control systems are coiled around the reality of everyday life. Recent years have seen a greater awareness to the importance of the critical infrastructure these control systems represent, as well as a heightened interest in protecting it. However, this activity does not necessarily mean that the critical infrastructure is really at risk, or that its control systems are really vulnerable to cyber attack. This chapter will examine these topics in order to establish the degree of risk that the critical infrastructure faces, particularly from the cyber threat, and the extent that control systems inherently contribute to that risk.

A. CYBER THREATS AGAINST CRITICAL INFRASTRUCTURE

The escalating rise in interconnectivity has dramatically changed the way the international community conducts political, economic, and personal business. Yet this connectivity comes with a price, and poses considerable danger to our nation's computer systems. The growing reliance on computers, and computer networks, within the CI industry makes those infrastructures vulnerable to eavesdropping, manipulation, and disruption by malicious individuals and organizations. This reality is not lost on the Federal Bureau of Investigation (FBI), which has classified seven major threats to our infrastructures. These threats could be considered singly or in any number of combinations, and are listed in Table 3.

The infrastructure of a Navy vessel is just as vulnerable to these threats as the national infrastructure. Naval warships are an important part of the American diplomatic and military presence abroad, and their mobility and capability for self-sustained operations make them ideal for global utilization. However, this also marks them as targets for a number of the adversaries listed in Table 3. For example, deployment to foreign waters places them into the sphere of influence of foreign intelligence services, making the exploitation of these vessels a top priority. Naval forces engaged in combat operations can fall prey to the enemy's information warfare attacks and find its capability to receive and process information degraded. Additionally, foreign and domestic

activists that are driven by environmental, pacifistic, or political motivations can view the presence of a U.S. warship as a symbol that represents the antithesis of their own ideology, and take steps accordingly to strike a blow in support of their beliefs. Naval vessels are not only vulnerable to hostile outsiders but can also carry their threats within their own hulls, as extreme conscientious objectors may seek to hinder the ship's participation in a mission that runs counter to their own personal convictions.

Table 3. Threats to Critical Infrastructures (From [1]).

THREAT	DESCRIPTION
Criminal Groups	There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.
Foreign Intelligence Services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Information Warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence,a can affect the daily lives of Americans across the country.
Insider Threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
Virus Writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and "worms" have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.

In all these instances, a ship can share the same threats, and the same vulnerabilities, as the nation at large. Since the processes of the national infrastructure are often replicated within a U.S. Navy ship, and the proper functioning of that ship is in the national in the national interest, then the critical infrastructure of that ship must be

considered a subset of the nation's critical infrastructure. Any examination of national critical infrastructure security must therefore intuitively include the ships of the Navy within its scope.

B. TRENDS IN COMPUTER ATTACKS

Since the critical infrastructure is permeated with computerized control systems, and since the protection of these infrastructures is gaining increasing attention, it seems germane to note recent trends in computer attacks. The Computer Emergency Response Team (CERT) Coordination Center at Carnegie Melon University has been investigating computer vulnerabilities and intrusions since 1988. Examination of the statistics compiled by the CERT indicates that concern about the safety of critical infrastructure control systems is not misplaced. The CERT reported a total of 38,016 known computer vulnerabilities due to software flaws during the period between 1995 and 2007, with over 6,000 more reported through the first three quarters of 2008. Additionally, the rates of these vulnerabilities have typically either been steadily rising or maintaining the same level during recent years [38]. Figure 11 provides the per-year breakdown of these reported vulnerabilities. Even though there was a drop in vulnerabilities between 2006 and 2007, the first two quarters from 2008 suggests that the upward will resume.

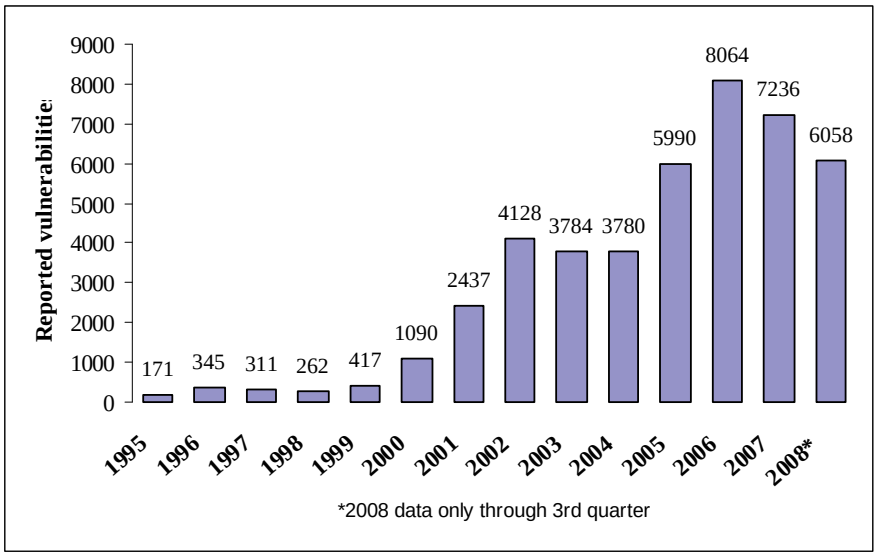

Figure 11. Reported computer vulnerabilities, 1995-2008 (After [38]).

The increase in computer vulnerabilities is significant because these flaws provide avenues that can be exploited to attack a system. Intrusion methods can be crafted to target particular system vulnerabilities, and the steady rise of vulnerabilities indicates a similar rise in potential attacks. Not surprisingly, computer incidents reported to CERT over the same period have risen dramatically in recent years. There were 315,749 reported computer incidents between 1995 and 2003, and the widespread use of attack tools has made these attacks so common that CERT no longer bothered to maintain a count after 2003. Figure 12 demonstrates the significant increase of reported incidents in recent years.

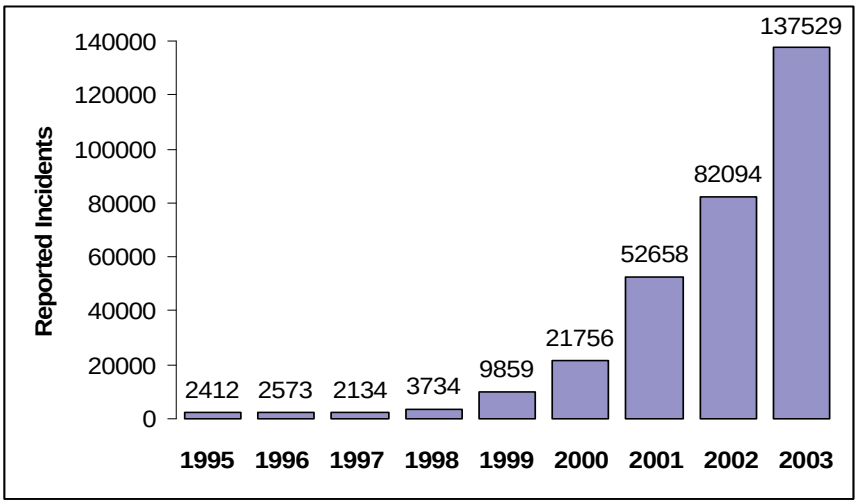

Figure 12. Reported computer incidents, 1995-2003 (After [38]).

The cost of these incidents is considerable. The 2007 Computer Crime and Security survey, conducted by the Computer Security Institute (CSI) and containing polling data obtained from 494 participating companies, reported that over 66 million dollars were lost as a result of some form of computer intrusion. The average financial loss for each of the respondents equaled $345,000, which more than doubled the average losses reported in 2006. In spite of this, the corporate world has not taken appropriate steps to combat this profligate monetary drain, with roughly 61 percent of the respondents reporting that their companies allocated 5 percent or less of the total IT budget to information security. Additionally, almost half of the companies spend less than one percent of their IT budget on security awareness, and while 46 percent of the

participating companies reported suffering a computer attack, only 29 percent filed a report with law enforcement agencies. Clearly, while computer intrusion is a costly problem, any attempt to combat this trend is hampered by the lack of cooperation by the corporate victims [39].

In the course of monitoring computer vulnerabilities and incidents, the CERT has noted six trends that indicate the likely direction computer attacks are heading. The sixth trend is particularly noteworthy with regards to this thesis, but all are applicable. These trends are discussed below.

1. Automation of Attack Tools

All of the techniques that hackers use in their efforts are becoming faster and more efficient, allowing the attack to occur with maximum impact. Reconnaissance of a target is typically conducted using social engineering or dumpster diving, but can be aided enormously if the attacker manages to insert surveillance software on a host. Automated scanning tools use more advanced scan patterns to spot potential vulnerabilities in target systems more quickly, and the vulnerabilities are often exploited as part of the scan itself, further increasing the speed of the attack. These vulnerabilities are largely due to "poor security practices and procedures, inadequate training in computer security, and poor quality in software products," and there is a preponderance of software that enables high-speed exploitation of flaws in order to gain illicit access [40]. Gaining access has been aided by the introduction of fast-spreading, self-propagating viruses like Code Red and Nimda, that can reach a point of global saturation in under 18 hours, at which point there is no longer any need for human intervention in the initiation of the attack [41]. Maintenance of illegal access and elimination of evidence of the attack are also automated though the use of backdoors or rootkits. These are software programs that allow intruders unfettered entry into the machine at will and grant the ability to manipulate the subverted machine so that detection of the presence of the attacker is much more difficult.

2. Increasing Sophistication of Attack Tools

The tools that hackers use to gain access are becoming increasingly sophisticated. Many of these tools are easily available for download on the Internet and do not require a great deal of expertise to use, resulting in instantaneous global proliferation and expanding utilization. Many hackers use tools that are resistant to computer forensics, making analysis difficult, and the attack patterns themselves are often random, defying attempts at signature-based recognition [41]. Additionally, these tools are becoming highly modular, so that attacks which used to implement only one type of attack are now polymorphic and capable of executing several different types of attacks. A further benefit of this modularity is the capability of an attacker to execute an attack across distributed systems, increasing the capability for saturating a target or widening the scope of an attack.

3. Faster Discovery of Vulnerabilities

As indicated in Figure 8, the number of computer vulnerabilities is increasing. Even in years when the rate of increase is the same or less than the previous year, the fact remains that there are still thousands of new vulnerabilities being discovered on an annual basis. Examination of software source code for a particular class of vulnerability often reveals instances of the vulnerabilities in hundreds of different software products, providing hackers with a ready-made target-of-opportunity list. Automated discovery of these vulnerabilities means that hackers are able to exploit them before vendors can correct them, and system administrators are usually unable to install software patches quickly enough to protect their systems from attack [41]. Even if they receive the patches in a timely fashion, administrators are often unwilling to apply them to their systems for fear of disrupting existing operations, and testing is conducted on a comparable system to observe the effects of the patch; this delay merely opens the window of opportunity wider for potential attackers [40].

4. Increasing Permeability of Firewalls

Firewalls are not as robust a defense mechanism as many people believe. According to the CERT, “technologies are being designed to bypass typical firewall

configurations; for example, IPP (the Internet Printing Protocol) and WebDAV (Web-based Distributed Authoring and Versioning)." [41] To make matters worse, many users and administrators believe their firewalls provide adequate security and allow themselves to be lulled into a false sense of assurance, providing even more opportunities for exploitation.

5. Increasingly Asymmetric Threat

By definition, the Internet is a network of networks. Because of this high degree of inter-connectivity, the basis of a system's security depends at least in part on the security of the other systems it interfaces with. This interdependency, and the development of distributed attack techniques, makes it easy for a single hacker to utilize many different machines to coordinate a highly effective attack. As trends in automation develop, and inter-connectivity continues to advance, the asymmetric nature of this threat will only increase [41].

6. Increasing Threat from Infrastructure Attacks

The CERT determines that there is a growing vulnerability for computer attacks to be directed against critical infrastructure targets. These attacks can take the form of distributed denial of service attacks, malicious introductions of worms into systems, attacks on the Domain Name Service (DNS), and attacks that specifically target routers [41]. As more and more people become more dependent on the Internet for the conduct of their daily lives, and as infrastructures become more and more dependent on computers for the execution of their function, the impact of these sorts of attacks becomes even greater.

These attack trends assume ominous significance when considered in conjunction with the SANS Institute placing improper user behavior on its annual list of top security vulnerabilities in 2006 and 2007. When coupled with human faults, the CERT attack trends indicate a potentially rich atmosphere of computer exploitation, and defending against such exploitation should be a matter of utmost importance.

C. THE THREAT OF CYBER TERRORISM

These attack trends are alarming once the dynamic new adversaries facing the country are taken into consideration. Potential enemies are no longer large nation-states but are smaller, more numerous, and infinitely harder to find. Their inability to muster a direct military resistance to the United States makes it necessary for them to implement alternate strategies to counter the American advantage in military power and technology. The events of recent years, including the attack on the *U.S.S. Cole* in Yemen in 2000, the World Trade Center attack in 2001, the wars in Afghanistan and Iraq, and the numerous terror incidents inspired by the heavy U.S. presence in the Middle East makes it highly likely that this concept of asymmetric warfare will continue. Attacks against critical infrastructures, and the computers that control those infrastructures, are just a few of the weapons that could be used in this type of warfare.

1. The Debate about Cyber Terrorism

There have been no confirmed accounts of terrorists either targeting computers for attack or directly utilizing them for an attack, and this has led to a considerable splintering of opinion regarding the likelihood of an effective terrorist cyber attack. Many critics believe that the terrorist threat against computer control systems is overstated. The considerable resources required to mount an effective cyber attack against critical infrastructures, that could take anywhere from two years to ten years to plan and execute, form a significant technological barrier against a catastrophic cyber strike [42]. Additionally, some people argue that the proprietary nature of many existing control systems will form another level of protection against exploitation, since a successful attack against one infrastructure would not necessarily provide any useful assistance to a second successful attack [43]. Furthermore, the very nature of terrorist attacks, that tend to focus on achieving maximum bloodshed and physical destruction in order to receive maximum publicity, may not translate well to a cyber attack that would probably be less spectacular in comparison. All of these arguments seem to indicate that terrorists are more likely to engage in a conventional physical attack rather than a computerized one.

However, the danger of a terrorist cyber attack cannot be overlooked. Although it is tempting to categorize terrorists as technically unsophisticated, the fact that computers were used to facilitate the planning of the September 11 attacks, and that there have been instances of using strong encryption to protect computer files, are indicators that they are no strangers to higher technology. Terrorist groups have demonstrated the capacity to make effective use of the Internet, which is ideal to utilize as a method of connecting affiliated groups who are geographically separated, since it supports operational redundancy and allows detailed information flow between the dispersed entities [42]. In addition, there is evidence that terrorist organizations such as Al Qaeda are definitely interested in the vulnerabilities of the U.S. critical infrastructure. A computer seized in Afghanistan contained structural analysis programs for dams, and there were indications that there was an increase in recent Web traffic relating to SCADA systems. Analysis of cyber attack data indicates that U.S. energy utilities are targeted far more frequently than other industries, and while these are mostly nuisance attacks, many of them emanate from the Middle East [42]. Compounding this problem is the fact that the power industry ranks near the bottom of all industries in providing funding for research and development compared to sales. Additionally, there are increasing load demands on electrical utilities, and the centralization and complexity of the power infrastructure as a whole leads to an infrastructure that appears to be a perilously ripe target [43]. All of these factors are potent indicators that the threat of terrorist action is a real one, and this must be taken into consideration when measuring the risk of an attack against critical infrastructures.

Military units in the Middle East are a constant target for terrorist operations. Improvised Explosive Device (IED) attacks against U.S. convoys, facilities, and personnel have been responsible for the greatest percentage, by far, of American military lives lost since the U.S. initiated Operation Iraqi Freedom in 2003. American military personnel also face a significant kidnapping threat, as evidenced by the abduction of a U.S. Army sergeant of Iraqi descent in 2005. As the *Cole* incident demonstrates, the Navy is just as vulnerable to terror attacks as U.S. ground forces, and given the wide range of terrorist actions that U.S. forces are subjected to, it is hardly beyond reason to think that electronic attack is beyond the realm of possibility.

2. Similarities between Hackers and Terrorists

Clay Wilson of the Foreign Affairs, Defense, and Trade Division notes that there appear to be many similarities between the tactics used to plan and execute a terrorist operation and those that are utilized to carry out a cyber crime [40]. This similarity of methodology may merely be coincidental, but the parallelism between the two groups is certainly striking. At a minimum, the comparison may provide insight into organization and techniques that are commonly used by radical groups, regardless of the nature of their extremism and the medium of their actions. However, the similarities may also indicate that the transition from physical to cyber terrorism is inevitable.

a. Organizational Structure

The structure of terrorist groups is not clearly understood, but what seems certain is that smaller groups are favored, organized in a non-hierarchal style. This allows concealment of the inner workings of the group, and also allows for quick mobilization for attacks, followed by a rapid dispersal to make detection and apprehension difficult. Similarly, hackers are usually individuals or small groups that meet anonymously in chat rooms to pass information about computer vulnerabilities and to plan ways to exploit them, and this means of gathering allows them to instantly disappear whenever authorities attempt to locate them [40].

b. Coordination of Strikes

One characteristic of many terrorist groups, Al Qaeda in particular, is the organization and execution of coordinated attacks. The hijacking of four planes at roughly the same time for the September 11 attacks, and the May 2003 attacks in Riyadh, are graphic illustrations of this tactic. Hackers have also made use of this tactic, crafting computer exploits that launch simultaneously from hundreds or thousands of infected hosts to produce calculated waves of disruption [40].

c. Pre-operational Surveillance

Terrorists typically conduct exhaustive preparatory planning prior to executing an attack. Hackers, as described previously, follow this same methodology when they footprint a target.

d. Motivated by Ideology

Terrorists are typically driven by some sort of ideological purpose, usually political in nature. Hackers share this trait, although the ideology may not be political. There are indications that more cyber intrusions are motivated by profit, but even this trend is ideological in nature.

e. Preference of Soft Targets

Hackers are opportunistic by nature, preferring to bypass hardened targets that are well defended and whose exploitation may not create the desired sensational effect [40]. Similarly, a growing hacking trend is to create a self-replicating Trojan horse or worm that can utilize known computer vulnerabilities, search the Internet for hosts with similar vulnerabilities, and then attack these soft targets where it can then be used in further exploitation.

D. CONTROL SYSTEM VULNERABILITIES

The threat posed by malicious individuals, whether ordinary hackers or cyber-terrorists, would merely be academic if the critical infrastructure was proof against exploitation. The determination of a control system's risk is a function of the determination of both threat and vulnerability. The presence of only one of these conditions means nothing. A fundamentally insecure system is in no danger if there are no threats poised to take advantage of its flaws, and a plethora of threats are powerless against a system that is proof against every attack levied against it. The statistical evidence of rising attacks against control systems demonstrates that the threat to the critical infrastructures is a significant one. Unfortunately, control systems are also rife with numerous vulnerabilities, making them susceptible to these attack vectors in a variety of ways.

As mentioned previously, some SCADA industry professionals focus their efforts on physical protection. This attitude is an exercise in tunnel vision. Physical protective measures are a necessary component of protecting control systems, because this defends against an attack that is easy to conceptualize, with a consequence of failure that is trivial to articulate. However, focusing exclusively on physical protection is woefully limited. The critical infrastructure's heavy dependence on computerized control systems renders it vulnerable to cyber exploitation, and failure to address this security shortfall could have potentially severe repercussions. A control system can be subjected to a Denial of Service (DoS) attacks, cyber-eavesdropping, or unauthorized access into the system. They can also be the victims of viruses, Trojans and Worms. All of these attacks can impact the principles of integrity, confidentiality, authenticity, and controlled access that a control system must possess in order to function in the face of a hostile environment.

Nevertheless, despite a decade's worth of recognition of these vulnerabilities, the problems of control system security persist. Investigations into these vulnerabilities have not led to significant progress in making these control systems more secure. The very properties that make these systems useful in administering the infrastructures that are so vital to the economic and social fabric of the nation are also the very reasons they are so vulnerable, and this contributes to the difficulty of the security problem.

1. Network-related Challenges

As mentioned in Chapter II, historical SCADA systems were part of standalone networks. However, the current trend is for these systems to become increasingly more interconnected with other networks. Many companies that utilize control systems are integrating these networks with their enterprise networks in order to increase the efficiency of operations and to allow for rapid transmission of real-time data to high-level personnel. Many of these enterprise networks offer connections to other networks, or to the Internet itself. This offers significant advantages for improved business operations, but also drastically increases the potential exposure of the SCADA network to malicious

threats. Connection to external networks often leads to the assumption that the external networks can be trusted, making the security of the control system dependent on multiple organizations [44]. Thus, the control system is only as secure as the weakest network it is connected to.

Since SCADA networks typically monitor an infrastructure that impacts large geographical area, remote components of these networks, such as RTUs and field devices, are generally widely dispersed. This necessitates the use of communications links that are either cabled or wireless. Sometimes these links are exclusively owned, but cost considerations make shared links more feasible. Information on these shared links could be extremely vulnerable to monitoring or manipulation, and users of the network may have an inflated degree of confidence in the security of the network links. Additionally, these remote components are often left untended for long periods of time, and a continual human presence is impossible to maintain, making them extremely vulnerable to physical attack. Physical security for these units is difficult to implement, and it has to be assumed that unauthorized personnel can gain access with relatively little difficulty [45].

The very nature of control system communications also contributes to the networking vulnerabilities. Control system communications are typically very small and very repetitive, and must be capable of real-time processing in order to effectively affect control over the network. Since these communications are often transmitted in the clear, they are ripe for exploitation. Traditional IT communications can be secured by encrypting the messages, but employing encryption in control systems poses a variety of challenges. These challenges include the difficulty of encrypting repetitive messages that are interspersed with occasional different messages, the necessity to support broadcast messages, the delay inherent in incorporating cryptographic operations, and key management. Because of the difficulty in finding solutions to these challenges without impinging upon stringent communications requirements, control system communications rarely utilize any sort of encryption [46]. In addition, the SCADA network often lacks a

well-defined security perimeter for the SCADA network, which results in spotty logging and auditing of control system communications traffic and the interleaving of non-SCADA traffic over the SCADA network.

Yet another problem with SCADA networks is their vulnerability to unauthorized remote access. These networks can contain many dispersed devices with access points that permit remote system diagnosis. The security for these access points is typically abysmal. Passwords are often poorly constructed and are usually transmitted in the clear. The network security policy may allow multiple devices to share the same password instead of establishing unique passwords for each device, thereby increasing the potential magnitude of network compromise. Passwords may be stored on the devices themselves for an indefinite period of time, and in some cases may not even be used at all [44]. This apathy to proper network security provides hostile intruders a golden opportunity to gain access into the system.

SCADA networks, that previously were almost completely dependent on proprietary protocols, have been recently migrating to utilizing standardized ones, and this has led to numerous additional vulnerabilities. Control systems are increasingly incorporating common protocols (like TCP/IP) and common transmission mediums (such as Ethernet, routers, and bridges), and the widespread publication of the vulnerabilities of these modern technologies makes security even more problematic for the SCADA system as a whole [44]. Additionally, many of these protocols are unsuitable for use in SCADA systems. TCP, for example, is a connectionless service that routes information packets based on determinations made by the individual routers, making it impossible to guarantee a dedicated, specified route. Network congestion can result in packet loss, and since TCP guarantees delivery of the packet, the attendant delay in having duplicate packets sent could introduce latency into a control system that must provide precision responses and cannot tolerate delay. The 802.11 wireless protocol is another widely-used common protocol that is not ideal for control systems, based on susceptibility of the protocol to denial-of-service attacks and the ease with which wireless packets can be captured.

2. Platform Vulnerabilities

Most SCADA systems are shifting from proprietary computer platforms to standardized commercial-off-the-shelf (COTS) platforms, such as Microsoft Windows and Linux, and this practice is contributing to the erosion of SCADA security. Like the open network protocols, many of these operating systems have well-known vulnerabilities, and the proliferation of readily available hacking tools provide a fairly easy way to exploit these vulnerabilities. To further complicate this matter, patches for these operating systems are not applied because of the uncertainty of disrupting control systems that are required to maintain continual operations [1]. Many of these operating systems are improperly configured for control system use and are installed with default settings, exacerbating the security problem by opening even more holes that potential attackers can exploit.

Since these platforms are often set up with default configurations that are rarely updated, they introduce security flaws throughout the SCADA system. Back-ups are often not stored for important platform configurations, so the devices are susceptible to critical information loss if a catastrophic service disruption occurs. Passwords are often poorly constructed and easily cracked, with no character length and character type requirements, and regular password aging is not enforced. Screensaver passwords are often not utilized, and many users may share a single password. In addition, normal users often have super-user or administrator privileges that provide them capability far in excess of what is required for the performance of their duties.

Systems often possess insufficient tools to detect and prevent unauthorized and malicious activity. Intrusion-detection and intrusion-prevention software is usually either underutilized, immature, or non-existent. Auditing and monitoring of system logs may not be done on a regular basis, and "malware" programs such as virus scanners may be out-of-date, unused, or completely uninstalled [44]. Additionally, the SCADA industries may fail to properly leverage the tools that they do have available. The vast amounts of data from security devices may overwhelm SCADA information security personnel and make monitoring attempts futile, and they "may only recognize individual attacks, rather than organized patterns of attacks over time." [10]

3. Administration Flaws

There is a tendency to treat control system security purely as a computer network problem; in reality, there are significant differences between normal computer networks and control systems. For example, control systems tend to be largely dispersed over a much larger geographic region than a regular network. The terminations of the SCADA network are usually fairly simple (and limited) sensors rather than general-purpose workstations. Communication among control system components, or to the master station, is usually on a report-by-exception basis, or a polled basis, whereas components of a normal network communicate as peers. Data packets tend to be small compared to regular networks. Unlike a normal network, SCADA networks are constrained by the requirement that it must function as specified under maximum load, and that system performance may not be impeded by security in any way. These differences mean that it is imperative that control system administration be developed separately from network administration, specifically tailored for the particular environment in which it operates [45]. Unfortunately, this does not often happen in practice.

Security administration for control systems is sadly underdeveloped. Few control systems are governed by identifiable security policies, and of those that are, even fewer include security administration that is specific to control systems [44]. Security procedures are few and far between. Control systems often have no security plans, security audits are rarely, if ever, conducted, and control system-specific security training is hardly ever performed. Another consequence of this somewhat haphazard administrative atmosphere is the fact that data within the control system is not usually assigned any sort of security level, making identification and classification of similar data types, and the enabling of appropriate areas to apply security precautions, impossible. This overall lack of security administration is fostered by the historical security-free environment of legacy systems, and perpetuates an atmosphere where security enforcement is disdained and security awareness is atrophied [44].

4. Public Availability of SCADA Information

Information about critical infrastructures and their control systems, as well as their associated vulnerabilities, is widely available via many open sources. This provides a mother lode of data that can be put to good use by potential attackers. The availability of this infrastructure and vulnerability data was demonstrated in 2005 by a George Mason University graduate student, who used unclassified material that was available publicly on the Internet while preparing his dissertation, which reportedly mapped every business and industrial sector in the American economy to the fiber-optic network that connects them [1].

This public information can be gleaned in a variety of ways, many of which are perpetrated by the SCADA industry itself. Many SCADA companies contribute to this gold mine by posting employee names, email addresses, corporate network names, and company organizational structure on the company's public web site, which provides an attacker a useful starting point. An intruder can obtain a reasonably thorough understanding of the power grid by utilizing a variety of publicly available documents and training aids, such as Federal Energy Regulatory Commission (FERC) orders 888 and 889, which mandates increased public access to electric power transmission system data [10]. Other public documents can allow an investigator to deduce load transmissions and identify critical nodes in the power grids. Data that is specific to control systems is easily available to anyone who is interested in it, and detailed information can be gathered about RTUs, system design documents, and technical standards for the interconnection of systems. Ordinary Internet processes can also assist the potential intruder in his preparation, since improperly configured DNS servers can provide IP addresses, server names, and email information as a result of zone transfers. All of this information could allow hackers to understand how the systems are constructed and to devise strategies to attack the weakest points of the systems.

Unfortunately, there is a larger pool of people poised to exploit this public information than ever before. The spread of publicly available exploitation tools, which CERT documented as one of the growing trends of computer attacks, has combined with a progressively computer-literate global population to greatly increase the number of

people capable of causing disruption to SCADA networks. Beyond the already-mentioned threat of hackers and cyber-terrorists, motivation to cause disruption to SCADA systems can range from disgruntled employees and ex-employees who are the victims of job cuts and downsizing, to disgruntled customers seeking reprisal as the result of inconvenient power blackouts and utility price increases. The wide availability of SCADA system operational network designs makes it easier for malicious entities to find network vulnerabilities, and since many leading SCADA systems are manufactured by global suppliers that market systems and distribute system documentation around the world, SCADA system information is now available to an even larger audience of potential troublemakers [10].

E. INCIDENTS AND ATTACKS AGAINST CONTROL SYSTEMS

Despite exhaustive government documentation, CERT's observations of increasing cyber attacks and growing ease of cyber exploitation mentioned in Chapter V, and the emergence of cyber-terrorism as a new potential "bad actor," there has been a mixed level of enthusiasm in the critical infrastructure industry to address control system security. A positive example is the SANS Institute, which is well known for conducting extensive information security training, certification and research, and frequently discusses CI security at classes, seminars, and conferences. However, the added cost of implementing layered security and conducting research into the development of SCADA-specific security has often reduced motivation for these pursuits with other representatives of the industry. Additionally, some industry representatives point out that there has been no single identifiable highly damaging cyber attack, and they believe that current industry procedures to recover from normal equipment outages and performance fluctuations would suffice to minimize damage from an intentional attack that they claim would be relatively localized and manageable. These representatives believe that the cyber threat to the national infrastructure is overstated, and prefer to focus their attention—and their limited resources—on physical protection [42].

However, this view is by no means universal. Other industry experts view this approach as short sighted, and they believe that corrective measures should be implemented before a catastrophic attack is launched. For example, interviews and discussions with representatives throughout the electric power industry caused the Information Assurance Task Force of the National Security Telecommunications Advisory Committee to conclude that "an organization with sufficient resources…could conduct a structured attack on the electric power grid electronically, with a high degree of anonymity and without having to set foot in the target nation." [1]

Clearly, there is great division within the critical infrastructure industry regarding the correct path to take. However, there are examples of control system incidents that clearly demonstrate that the potential for SCADA disruption certainly exists. It is important to note that this disruption does not need to be the result of calculated hostile action—an environmental disaster, improperly configured server, or poorly written program can have much the same effect as a planned attack. This makes the debate over the existence or capability of an adversary almost moot. The historical examples given below, from both the DoD and civilian sector, encompass both accidental and premeditated disruptions. They transcend theoretical studies and government directives because they provide cold, empirical evidence that the cyber threat to control systems is genuine, and demonstrate that failing to address control systems security shortfalls will surely result in more frequent incidents, with more calamitous results.

1. Simulated Exploitation of U.S. Electrical Power Grids

Illustration of the vulnerabilities of the nation's critical infrastructures occurred as early as 1997 during a military exercise called Eligible Receiver. During this exercise, personnel from the National Security Agency (NSA) demonstrated how easily they could have subverted the nation's electrical power complex using tools that were easily obtainable from the Internet. The group of 50 to 75 hackers demonstrated that they could have shut down electrical power throughout the nation, as well as disrupting command-and-control elements of the U.S. Pacific Command, leaving the nation in the dark and severely crippling a sizable portion of American military capability [47].

2. USS YORKTOWN Calibration Flaw

The USS YORKTOWN suffered an engineering LAN casualty that caused the entire LAN to crash, leaving the Aegis cruiser dead in the water for three hours near Cape Charles, Virginia. This casualty was the result of a maintenance petty officer entering a faulty data value of "zero" in the ship's database. Although the incident was accidental, without malicious intent, and was the result of manually inserted data rather than a cyber-related attack, it demonstrates the potential opportunity for misuse that these systems possess [48].

3. Arizona Roosevelt Dam Incident

A twelve-year-old boy, for no other reason than curiosity, successfully penetrated the computer systems that control the Roosevelt Dam in 1998. The hacker had no ill intent and was not interested in manipulating the dam once he had completed his intrusion, but he had complete command of the control system controlling the dam's massive floodgates, which hold back as much as 1.5 million acre-feet of water, or 489 trillion gallons. That volume could theoretically cover the city of Phoenix, down river, to a height of five feet. This would not have happened in actual practice, since the water would spend most of itself in a flood plain before it reached the Arizona capital. However, the flood plain does encompass the cities of Mesa and Tempe—with a combined population of nearly a million. Physically destroying a dam would require literally tons of explosives, but it is obviously possible to perform a similar breach through cyberspace [49].

4. Washington Gas Pipeline Rupture

A 16-inch-diameter steel pipeline owned by Olympic Pipe Line Company ruptured and released 237,000 gallons of Gasoline into a creek in Bellingham, Washington. The gasoline ignited, severely damaging the city's water treatment plant, destroying a single-family home, causing approximately $45 million dollars in property damages, and killing three people. Among the many factors that contributed to the rupture was the company's practice of conducting database development work on the SCADA database while the system was being used to operate the pipeline, resulting in a

critical period of non-responsiveness during the time of the rupture. As with the case of the USS YORKTOWN, this was not a case of sabotage, or even a case of control system failure, but it is easy to surmise how a cyber attack that rendered the control system inoperative, coupled with a coordinated deliberate physical rupture of the pipeline, could replicate this incident and inflict significant havoc [50].

5. Australian Sewage Release

In Queensland, Australia, on April 23, 2000, Vitek Boden was arrested by police in his vehicle as he prepared to conduct a cyber attack against the control systems for the Maroochy Shire wastewater system. Boden, a former employee of the firm who supplied Maroochy Shire with its remote control and telemetry equipment, had perpetrated 46 successful attacks against the system before his arrest, releasing considerable amounts of sewage into parks, rivers, and a hotel, causing severe environmental harm. His goal was apparently to be hired as a consultant to correct the problem he had created. During his intrusions, Boden was in complete command of over 300 nodes that governed both fresh water and wastewater, and could have created considerably greater calamity than he chose to exert [49].

6. Slammer Penetration of Nuclear Power Facility

Ohio's Davis-Beese nuclear power facility was penetrated by the Slammer worm in January of 2003, disabling the safety monitor system for a period of 5 hours. The worm entered the system through the unsecured network of an unnamed Davis-Besse contractor, which was bridged to the Davis-Besse corporate network. This connection was one of multiple ingresses into Davis-Besse's business network that completely bypassed the plant's firewall, which was programmed to block the port Slammer used to spread. Once inside the business network, the worm entered the electrical plant network through an unpatched MS-SQL vulnerability, and the congestion caused by its activities caused the plant network to crash. The facility had a redundant analog system that ensured that power delivery was uninterrupted during the time the monitoring system was disabled, but this incident illustrates the capability that even an undirected attack can possess [51].

7. August 2003 Blackout

Parts of the northeastern United States, as well as eastern Canada, suffered the largest blackout in North American history on August 14, 2003, when electrical power was disrupted for approximately 50 million people. The cascading effect of the blackout has been attributed to the spread of the Blaster worm, which broke out approximately three days prior to the blackout, and which may have inhibited communications on computers that are used to monitor the power grid. Economic impact of the blackout has been estimated to range from $6 billion to $50 billion [1].

8. 2008 CIA Assertion of Multi-City Attack

On January 16, 2008, a senior CIA analyst claimed that there had been multiple instances of cyber intrusion into utilities systems outside the United States. The analyst made these claims at the SANS Institute Process Control Security Summit in New Orleans, while speaking to an audience consisting of national government officials from four countries, engineers and security managers from many North American utilities, and other critical industry asset owners from all across North America. Extortion accompanied the intrusions, and on at least one occasion, a disruption was initiated which caused a power outage affecting multiple cities [52]. Although the cities were not identified and no further information was forthcoming, the claim does substantiate the vulnerabilities of utility SCADA systems.

The multitude of attack vectors, coupled with significant vulnerabilities and historical examples of control system disruption, demonstrate that the risk to control systems is very real. The vulnerabilities of control systems are a cause of growing concern and pose a serious problem to the critical infrastructure. Most of the problems are technical in nature, but some, such as the resistance to apply proper security administration and the prevalence of open-source information, are based on the culture of the SCADA industry. Control systems are fraught with significant vulnerabilities and riddled with enormous security implications. The systems used on Navy ships are no

less at risk, and no less vital, than their counterparts in the national critical infrastructure. Chapter VI will examine some of these security concerns and determine if those systems share the vulnerabilities of their civilian cousins.

VI. A LOOK AT SHIPBOARD CONTROL SYSTEM SECURITY

Despite some obvious similarities, shipboard control systems differ considerably from their civilian counterparts, as mentioned previously. Control systems can vary from ship to ship, with a variety of different systems and applications being utilized perform similar tasks. Shipboard systems also combine the "traditional" monitoring and control of utility functions with the monitoring and control of ship combat systems, which has no analogue in the civilian SCADA industry. In general, national CI control systems seem to be specialty systems, while shipboard control systems appear to be more general-purpose.

In addition to these functional differences, it must be noted that the very mission of a warship routinely places it in situations where it may be subject to physical damage, either from rough seas, inclement weather, or enemy combat action. Hence, its control systems are indirectly placed in harm's way far more frequently than a civilian CI system. Shipboard control systems also tend to operate in environments of significant physical stress and are subject to physical challenges that civilian CI control systems do not usually encounter. A prime example of this threat is the occurrence of fire within the tightly-confined compartments of a board ship. Shipboard control systems can also be at risk for intense water damage due to the possibility of flooding, either from their compartments becoming open to the sea or from firefighting efforts in their area. Additionally, the proximity of shipboard control systems to salt water and other corrosive agents can make them easier targets for physical degradation. In all cases, shipboard control systems face a much more diverse physical challenge then their civilian counterparts.

However, despite these differences, both critical infrastructure and shipboard control systems share similar attributes. Both are at risk to be targeted for exploitation by hostiles, and exploitation against both is facilitated by similar circumstances. Both types of control systems can have similar susceptibility to the automation and sophistication of attack tools, the rapid discovery of vulnerabilities, the permeability of intrusion-detection

systems, and the emergence of the asymmetric threat of terrorism. Finally, both exert considerable influence on the critical infrastructure they manipulate, and the criticality of protecting both is self-evident.

A. WEAKNESSES IN FEDERAL INFORMATION SYSTEM SECURITY

However, it has proven impossible to determine whether shipboard control systems are secure, or to even make a qualitative expression of their security. The scope of this issue, and the variety of equipment configurations within the Navy, make such a statement impossible. It would be necessary to examine every ship in the Navy to make an accurate determination. However, inference can be made by examining how federal government information systems fare in several of the typical categories applied during vulnerability assessments.

1. Certification and Accreditation

The Federal Information Security Management Act of 2002 (FISMA) mandates that all federal agencies, including the DoD, must enact measures to buttress the security of the information systems used by those agencies. FISMA also establishes a framework that ensures the effectiveness of the information security controls that are implemented over federal information assets. These regulations apply to control systems as well as normal IT systems. The criteria that will be used in conducting this high-level assessment are based loosely on the guidelines promulgated in NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems,” which satisfies the requirements laid out in the FISMA. Detailed IA controls for control systems can be found in Appendix I of this publication.

One of the methods that the DoD Information Assurance Program articulates to implement the FISMA mandate is to require product specification and evaluation in accordance with the Common Criteria [53]. In order to determine the security of a control system, there must be a way of expressing the level of security that the control system possesses. This is true for CI control systems, as well as the control systems on a Navy

ship. Certification and accreditation (C&A) is a way of formulating this expression, and any notion of securing shipboard control systems must begin with a strong C&A program.

The initial steps of this specification and evaluation process is to determine the system boundaries, information types, responsible individuals, interconnections with other systems, and implementation details for various security controls. Once a system is properly defined and thoroughly documented, the next step is to perform certification and accreditation of that system. Certification is a thorough security evaluation that encompasses all aspects of an information system's physical, personnel, administrative, information, and communications security, in order to determine the degree that a specific design and implementation meets a specified set of security requirements. Accreditation is a formal decision by a designated third-party approving authority that the information system being examined is authorized to operate in a specific operating environment.

C&A is mandatory to determine those DoD systems that may be allowed to operate, and thus is vital for providing a reasonable level of assurance that the security functions of a product performs as the designers of the product claim. Two processes are currently used within the DoD to accomplish certification and accreditation, and both will be examined in brief.

a. DITSCAP

Until recently, certification and accreditation within the DoD was conducted according to the DoD Information Technology Certification and Accreditation Process (DITSCAP). Designed to secure and protect all of the entities within the Defense Information Infrastructure (DII), the DITSCAP was designed to provide standardized activities that, when completed, will lead to a successful certification and accreditation of an IT system. It was applicable to the acquisition, operation and maintenance of any DoD IT system that collects, stores, transmits, or processes unclassified or classified information. These systems could be newly developed systems, prototype systems, IT systems that were already incorporated into an infrastructure, reconfigured or upgraded

systems, and legacy systems [54]. Although the DITSCAP contained mandatory activities, it was designed to be tailored in order to adapt to various types of system, computing environments, and missions.

Changes in the utilization of DoD information systems, as well as requirements articulated in the DoD Information Assurance policy, demanded a revision in the DoD C&A process. The DoD Information Assurance (IA) policy is designed to embrace a net-centric information architecture through the enforcement of IA controls that establishes baseline requirements for information availability, integrity, and confidentiality. The DITSCAP was incapable of meeting the requirements of the new information system architecture and did not address concepts and specifications that were articulated in DoD IA policy. Hence, DoD C&A is in the process of transitioning from the DITSCAP to the DoD Information Assurance Certification and Accreditation Process (DIACAP).

b. DIACAP

The concept of a Global Information Grid, commonly referred to as the GIG, completely altered the way the DoD utilized information technology. The GIG is a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel that is used for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. It supports all DoD, national security, and related Intelligence Community missions and functions and provides capabilities from all operating locations, as well as interfaces to coalition, allied, and non-DoD users [55]. The GIG concept eliminates the notion of individual systems with the concept of a net-centric information-sharing environment, which requires that information is not only visible, accessible, and understandable, but also posted to shared spaces and tagged for easy discovery. The net-centric concept also mandates that information must also be organized within dynamic Communities of Interest that may require the transmission of data across traditional system and classification boundaries in support of operational necessity [56]. While this sort of architecture vastly enhances the sharing of information, it is also inherently vulnerable to

exploitation and denial of service. It therefore requires a dynamic and flexible C&A process that could not be fulfilled by the DITSCAP.

The DIACAP overcomes many of the characteristics of the DITSCAP that rendered it unsuitable for utilization within the new DoD IA policy. The DITSCAP generated security requirements and metric data that was system-unique, and was a manual, time-consuming process that often lacked current and complete information on the system. In addition, it did not apply the principles articulated by FISMA and did not evaluate the baseline IA controls described in DoD IA policy. In contrast, the DIACAP implements required IA controls across all DoD systems in compliance with FISMA, while at the same time providing improved support to certification personnel and enhancing the usability and reusability of C&A products. It supports the transition to the GIG architecture by ensuring a uniform C&A approach that is able to accommodate different systems and operate in a dynamic environment. A brief comparison of the DITSCAP and DIACAP is shown in Table 4.

Table 4. DITSCAP & DIACAP Compared (After [56]).

DITSCAP	DIACAP
Security requirements and standards uniquely determined by each system	All systems inherit enterprise standards and requirements
Policy advocated tailoring, but process was hard-coded to phases	No pre-defined phases. Each system works to a plan that aligns to the system life cycle
Accreditation status communicated via letter and status code (ATO, IATO) in SSAA	Accreditation status communicated by assigned IA Controls' compliance ratings, and letter and status code (ATO, IATO, IATT, DATO) in DIACAP Scorecard
No process improvement	Automated tools, enterprise-managed knowledge base, requirements tied to architecture
Inaccurate association of ATO with perfect and unchanging security	ATO means security risk is at an acceptable level to support mission and live data
"Fire and forget" accreditation; 3 year "white glove inspection" re-accreditation	Continuous, asynchronous monitoring; reviewed not less than annually, FISMA reporting

The DIACAP embraces the net-centric concept by utilization of online applications such as the DIACAP Knowledge Service (KS) and Enterprise Mission Assurance Support Services (eMass), which are used to support the C&A effort. The Knowledge Service is a web-based repository of C&A information. It contains C&A guidelines, diagrams, and documents that can be utilized as an aid to DIACAP execution. It also serves as a C&A collaboration community where DIACAP users can be exposed to lessons learned and best practices, implementation guidance, expected results of IA controls, and the latest information assurance news. eMass is a scalable, flexible online suite of information assurance management tools that is used to create a C&A package for registering all systems undergoing C&A and to monitor the progress of the each system as it moves through the C&A process. An important part of eMass is the DIACAP ScoreCard, which is a summary report that shows the implementation and validation status of an information system's IA controls and which communicates the accreditation decision.

c. Questions Regarding the Application of C&A

Although statistical data may indicate otherwise, certification and accreditation throughout the federal government—including the DoD—lacks cohesion and uniformity. The average percentage of federal IT systems authorized after certification and accreditation, as reported by 24 federal agencies, was 62 percent at the end of the Fiscal Year (FY) 2003 and 77 percent at the end of Fiscal Year 2004, which marked the beginning of a substantial upward trend [57]. This percentage has risen each year, culminating with a federal accreditation rate of 92 percent for all federal systems following Fiscal year 2007, which would seem to indicate an impressive rate improvement in the C&A of federal systems [58]. However, this percentage still falls short of the universal compliance mandated by both the DITSCAP and the DIACAP, and factors other than raw numerical data may provide a more accurate picture of the C&A landscape

Examination of the polling data over the past four years shows that this reporting is highly suspect for a variety of reasons. One such reason is the lack of a clearly-defined statistical population from which to generate accurate statistical data. Some agencies include both non-national security and national security systems in their reported performance data, while others do not. Additionally, some agencies—specifically DoD—include systems with interim authorization to operate among those systems reported as certified and accredited, while other agencies only report systems with complete and final accreditation [59]. Further complicating this picture is the inability of some federal agencies, namely DoD, to compile a complete and accurate inventory of their major information systems. The DoD's failure in this regard is due in part to the lack of a uniform definition of what precisely constitutes an information system, and the subsequent necessity for each Defense component to "make independent interpretations of whether the asset under evaluation should be reported as a system for FISMA purposes." [60] Such variance in statistical populations across federal agencies makes it impossible to accept the accuracy of reported C&A rates at face value and brings the validity of the data into question.

Aside from the uncertainty of the populations used to gage C&A completion, there are other C&A concerns. Compliance information for FY 2004 was gleaned directly from the agencies, with no third-party verification of the facts, which clearly introduces uncertainty with the accuracy of the data for that year. Additionally, inspector generals (IG) of the federal agencies have historically noted problems with the quality of the C&A process itself, with the percentage of agencies that were evaluated to have unsatisfactory certification processes, ranging from a high of 40 percent in FY 2004 to a low of 25 percent in FY 2008. Complicating this issue, is the lack of a common approach for FISMA evaluations, resulting in considerable differences in the scope and methodology of the evaluations across federal agencies [58]. Clearly, these discrepancies skew the data in the reports, and demonstrate that the C&A process is still a work in progress.

2. Access Controls

Access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. One method of access control is user identification and authentication, which enables a computer system to uniquely identify users and to validate a user's claimed identity. Assigning users the proper access rights and file permissions, which enforces the principle of granting a user the minimum privileges necessary to perform his or her job, is another type of access control. Yet another form of access control is to establish individual accountability, monitor compliance with security policies, and investigate security violations, all of which are accomplished through the use of auditing software. Other forms of access controls include controlling who can implement software changes, ensuring proper segregation of duties, and protecting computer facilities and resources from espionage, sabotage, damage, and theft. It is critical to utilize proper access controls in order to ensure the proper operation and availability of an information system, as well as to protect the integrity of the data stored on, and transmitted by, the information system. Failure to do so places federal information systems at considerable risk of fraud, misuse, and disruption [61].

Unfortunately, most major federal departments have had significant difficulties addressing deficiencies with their information system's implementation of access controls. According to GAO reporting, 23 of 24 major agencies had major access control weaknesses in FY 2004. These weaknesses included problems with mismanagement of user accounts, improper structure of passwords, and inappropriate access rights, with 22 of the major agencies demonstrating weak software change controls, while 14 agencies failed to properly segregate information security duties [61]. This unfortunate trend carried over into FY 2005, with 14 federal agencies reporting significant deficiencies in the design or operation of internal controls, and 6 agencies reporting material weaknesses in their information systems, that prohibited them from providing reasonable assurance that data inaccuracies, or even complete loss, could be prevented or detected on a timely basis [62]. The following years were not much better, as FY 2006 and FY 2007 showed access control non-compliance rates of 92 percent and 96 percent respectively.

These weaknesses spanned the entire spectrum of access control. For example, users were often not compelled to create strong passwords that had a minimum length greater than zero, and instead created passwords that were common words, increasing the possibility that an attacker could guess the password and gain access to the account. In some cases, passwords were vender-default, or were shared among users. Flaws in software change control included failure to ensure approved and correct software updates with appropriate documentation. Several agencies improperly managed user accounts by imprudently granting users excessive access permissions, that allowed them to create or change sensitive system files, while unused accounts were not always deactivated when personnel transferred, or no longer required access. Segregation of duties was another area where agencies failed to separate duties and responsibilities, such as those performed by system administrators and security administrators, in a manner that ensured the isolation of incompatible functions. Fictitious users at one agency could be added to a system with enhanced access permissions, and would be empowered to perform unauthorized activities undetected, while another agency allowed financial transactions to be both initiated and approved by the same individual. Agencies also struggled with configuring remote access, allowing simultaneous connection to both the Internet and the internal network, and failing to restrict external communication traffic, which could result in an attacker remotely controlling the Internet sessions of legitimate users, or launching attacks against sensitive network devices. Finally, agencies had several failures regarding the monitoring of security events, including the lack of automated preparation of security reports in response to security-related events such as failed login attempt reports. All of these failures indicate that the federal government as a whole lacks the ability to ensure that access to, and manipulation of, its information systems is restricted only to legitimate individuals.

3. Physical and Environmental Protection

In addition to other forms of access control, physical protection of information resources was a problem with many federal agencies. Many agencies had virtually no effective physical barriers to access, with visitor screening procedures that were either inconsistently implemented, or entirely absent. For example, the Federal Deposit

Insurance Corporation (FDIC) did not always apply physical security controls for some instances, allowing an unauthorized visitor to enter a key FDIC facility "without providing proof of identity, signing a visitor log, obtaining a visitor's badge, or being escorted." [63] Departments also struggled with controlling access among its own personnel. One agency allowed several individuals access to sensitive areas without properly justifying a need based job duties, and did not remove physical access authorizations into sensitive areas in a timely manner for employees who no longer needed it to perform their jobs. This paled in comparison to another department, which granted "over 400 individuals unrestricted access to an entire data center—including a sensitive area within the data center—although their job functions did not require them to have such access." [64] In FY 2006 in particular, federal agencies noted a rash of security incidents that resulted in the theft, loss, or improper disclosure of personally identifiable information on millions of Americans, mostly as the result of physical thefts or improper safeguarding of systems. The Internal Revenue Service (IRS), Federal Aviation Agency (FAA), and Federal Bureau of Investigation (FBI) were among the departments to suffer weaknesses in their ability to physically protect their information systems.

The federal government has attempted to correct at least part of this problem. In recognition of the variations in the forms of federal identification, and in an effort to increase the quality and security of identification practices across the federal government, President Bush issued Homeland Security Presidential Directive 12 (HSPD-12) in August 2004 to establish a mandatory, government-wide identification standard. In response, the National Institute of Standards and Technology (NIST) issued the Federal Information Processing Standards (FIPS) Publication 201, designed to provide improved identification and authentication of all federal employees and contractors in the form of "smart cards." However, as noted by GAO in 2006, many federal departments have encountered challenges in implementing this standard. These challenges include uncertain program costs that preclude proper budgeting; an inability to test and obtain compliant smart cards and card readers within mandated deadlines; confusing guidance promulgated by NIST that has led to multiple approaches which could may delay smart

card interoperability throughout the government; and incomplete guidance regarding precisely which facilities, people, and information systems fall under the mandate of FIPS 201 [65]. These problems stretched into 2008, with agencies making only limited progress in implementing and using smart cards. None of the agencies examined by GAO met established deadlines for issuing smart cards, and of those agencies that had issued smart cards, most had not been using the electronic authentication capabilities on the cards and had not developed implementation plans for those authentication mechanisms [66]. These problems are only a small part of the physical protection issue of shipboard control systems, but given the automated nature of today's military, it seems correct to note that the difficulties with personal identification and verification underscore the difficulties with physical security as a whole.

4. Security Assessments, Awareness, and Training

The Office of Management and Budget (OMB) requires that all federal agencies must conduct a periodic security assessment of the overall security controls that are employed by that organization's information system. This security assessment is designed to determine the extent to which the management, operational, and technical controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system [67] The periodicity of this assessment can vary, but should not be less than annually.

As is the case with certification and accreditation, data gleaned from annual federal reports to the OMB paints a rosier picture of the state of periodic testing than the raw data would indicate. The percentage of federal systems that underwent annual testing has oscillated wildly from 2003, with major gains being made in 2004 followed by alternating ebbs and increases every year since. FY 2007 reports a robust assessment rate of 95 percent, but this number conceals problems lurking beneath the surface. For example, "11 IGs reported that their agency did not always ensure that information systems used or operated by a contractor met the requirements of FISMA, OMB policy,

NIST guidelines, national security policy, and agency policy. In addition, two IGs reported that agencies did not conduct their annual assessments using current NIST guidance." [68]

These findings corroborate a comprehensive GAO examination that was conducted to determine whether federal agencies adequately designed and effectively implemented policies for the periodic testing and evaluation of information security controls. GAO surveyed 24 federal agencies to determine if effective policies had been designed, by analyzing their policies to verify if they included elements important for conducting effective tests and evaluations. GAO also examined how well six of these agencies implemented their policies, by inspecting the methods and practices that were used to test and evaluate controls for 30 of their systems.

This investigation revealed substantial problems with all 24 agencies. Every agency failed multiple criteria that GAO used to judge the design of their policies. Every agency had inadequately designed testing and evaluation policies. All 24 agencies that were surveyed failed multiple criteria that were used to evaluate their policies. For example, many agencies did not properly identify and test security controls common to multiple systems. Others did not clearly define the roles and responsibilities of personnel performing tests, or the frequency of their periodic testing. None of the agencies' policies addressed how to determine the depth and breadth of testing according to risk, and one agency had no policy whatsoever. Additionally, GAO's review of the 30 information systems revealed that the methods and practices for testing and evaluating controls at the six case study agencies were inadequate in providing reasonable assurance that consistent assessments of similar quality could be achieved by repeated evaluations. These agencies suffered from insufficient documentation to support testing methods and results, undefined assessment methods that were to be used when evaluating security controls, and failure to include remedial actions in testing plans [69].

The DoD has been specifically cited as a department that had particular challenges in this regard, despite achieving a gaudy testing and evaluation rate of almost 88 percent between 2003 and 2006. The DoD did not clearly define the roles and responsibilities of personnel performing tests, and also failed to specify the identification

and testing of common security controls. The DoD also lacked instructions for selecting minimum security controls evaluated during periodic testing, as well as determining the depth and breath of testing. Finally, security control testing was not performed consistently across all DoD components [68].

All personnel within the Department of the Navy (DON) are required to meet certain minimum-security training requirements. These are documented in DoD Directive 8570.1 and Secretary of the Navy (SECNAV) Instruction 5239.3A. Both documents indicate that all personnel using DoD or DoN information systems, as applicable, are required to have basic security awareness training. Additionally, those personnel whose duties require privileged access to the systems must have specialized training commensurate with their duties.

Annual reports to OMB indicate that federal security awareness training is not as robust as one might hope. The overall percentage of federal employees who received basic security awareness training has fluctuated up and down since 2003, and although agencies reported a training percentage rate of 84 percent in FY 2007, "eight agency IGs disagree(d) with the percentage of individuals that their agency reported as having received security awareness training," including six agencies that reported training rates between 96 and 100 percent [68]. The DoD in particular has difficulty with accurate verification of who among their widely dispersed user base has received the required awareness training, as well as monitoring those individuals who perform security-related duties, and are thus required to receive specialized training [60].

Despite these difficulties, the figures are more positive with regards to specialized training. The percentage of employees with security-related responsibilities who received specialized training has steadily risen since FY 2005, and FY 2007 documented an impressive specialized training rate of 90 percent [68]. This indicates that the training environment is far from barren. However, until the DoD and other challenged departments develop solutions to their training issues, the actual percentage of personnel who have received the proper training cannot be accurately ascertained.

5. Personnel Security

An important consideration of personnel security is the assurance that personnel filling designated positions have been properly screened prior to assuming duties that may expose them to sensitive information. In the DoD, this screening often takes the form of a security clearance, which is generally used to determine the level of information an individual may have access to. There have been sizable problems with the DoD's personnel security clearance program in recent years, of a magnitude sufficient for GAO to judge the issue as a high risk area [65]. These problems can adversely impact the personnel security that surrounds DoD information systems, including control systems, either by placing uncleared personnel in the proximity of sensitive information, or by forcing cleared but unqualified personnel to assume positions of trust they may not be prepared for.

The DoD's problems were first noted by GAO in 2005 and have continued to the present day with minimal correction. The most significant difficulty lies with the lengthy amount of time required to grant a clearance. In January and February 2006, clearance processing time was an average of 286 days for initial clearances and 419 days for clearance updates [70]. By contrast, the end-to-end processing of initial top-secret clearances that was reported in August 2007 took an average of 276 days, while renewal of top-secret clearances required 335 days—an improvement, but still far in excess of the goal of 120 days [65]. These delays are exacerbated by the lack of full reciprocity between government agencies regarding the granting of clearances, resulting in duplicative investigations and adjudications among agencies. This lack of reciprocity is the result of agencies' concerns that other agencies may have conducted inadequate investigations during the clearance process. This implies that there have been significant issues in the past that certainly puts sensitive information at risk. Yet another problem was the DoD's chronically inaccurate projections of expected clearance requests, which negatively impacted man-hour planning and cost expectancies. All of these challenges illustrate a lack of assurance in the DoD's personnel security program, which has an obvious attendant effect on the security of information systems in general and control systems in particular.

6. Transition to Wireless Networks

A recent technological trend is the incorporation of wireless networks in shipboard control system networks. Although there are installation and cost benefits associated with wireless networks, these networks are still subject to the same security risks that are associated with conventional wired networks, as well as problems that are specific to the wireless networking environmental. Since wireless networks broadcast information via radio waves that propagate between 150 feet to 1,500 feet, signal leakage can result in information being exploited by attackers more easily than in a conventional wired network [71]. Wireless network vulnerabilities can be mitigated by the development of policies that define requirements and establish security controls; by the use of wireless security tools such as encryption, authentication, virtual private networks (VPNs), and firewalls; by the implementation of comprehensive wireless network security monitoring programs; and by fully training personnel on appropriate wireless networking security policies.

However, the federal government has faced significant problems in meeting the challenges inherent in wireless networking. Many agencies have not developed policies addressing wireless networks, and of those agencies that did have policies, many of them did not include an acceptable use policy. Over half of the agencies surveyed by GAO in FY 2005 did not have configuration requirements for wireless networks, and the configuration requirements of the other agencies often lacked key elements such as the use of and settings for security tools such as encryption, authentication, VPNs, and firewalls; proper placement and strength of wireless access points to minimize signal leakage; and the physical protection of wireless-enabled devices [71]. Even those agencies with proper configuration requirements likely had problems executing them—in addition to the federal government's aforementioned problems with authentication, federal agencies also face significant challenges with encryption and VPNs that range from improper configuration, inadequate training, and incomplete policies [72]. Most of the major agencies did not establish comprehensive wireless network monitoring programs for detecting signal leakage, and 75 percent of the agencies surveyed did not have any training programs on wireless security or the policies. GAO testing of the

wireless network security of six federal agencies identified significant weaknesses related to signal leakage, configuration, and unauthorized devices [71]. Fortunately, all is not lost regarding federal wireless networks, since the Defense Information Systems Agency has published Security Technical Implementation Guides to be used in hardening wireless networks. However, properly securing wireless networks should continue to be an area of attention, since failure to do so would pose a serious risk to the confidentiality, integrity, and availability of the information contained on federal information systems.

B. ASSESSMENT OF SHIPBOARD CONTROL SYSTEMS

DoD information systems share, at least in some degree, the flaws exhibited in the federal information system as a whole. It can thus be inferred that the information systems of DoD components (such as the Navy) likely suffer from similar problems that are symptomatic of federal information systems. Shipboard control system security will now be looked at in a general sense, based upon personal observation on board the *U.S.S. Paul D. Foster*, and from other documentation uncovered by research.

1. Certification and Accreditation

In light of the problems previously detailed concerning certification and accreditation within the federal government and the DoD, it is perhaps not surprising that research for this thesis revealed a paucity of evidence that control systems within the DoD are routinely subject to either the DITSCAP or DIACAP. Interviews with members of the U.S. Navy engineering community, indicate that many personnel are not even aware that SCADA-like systems are employed on U. S. Navy vessels, despite occupying positions that should have made them privy to such information. Communication with information technology professionals attached to the Space and Naval Warfare Systems Command (SPAWAR), at both the San Diego and Charleston centers, was initiated in the hopes that these agencies could provide documentation of the existence of, and certification and accreditation of, control systems on board ships. The personnel at both SPAWAR centers were not only unable to find any case of an SSAA submitted for shipboard control systems, but were also unable to determine whether these systems existed in the first place. These events are not recounted to imply that C&A is non-

existent for shipboard control systems—not only is such a claim clearly unsupported but is also untrue, since research did manage to unearth one SSAA for a shipboard HM&E system. However, one C&A example does not indicate a trend, and the difficulties in finding other examples illustrate that the U.S. Navy C&A process for shipboard control systems perhaps suffers from the same lack of cohesion that is evident throughout the federal government.

2. Access Controls

In some cases, shipboard control systems appear to satisfy some of the guidelines for appropriate access control. The Integrated Condition Assessment System (ICAS) demonstrates this. For example, user rights are separated based on one of four roles that a user is assigned, and these roles are governed by the "least privilege" principle. A normal user may access all standard display and database functions, make manual log entries, and create limited bitmap files depicting a graphical representation of a system or component. However, they have no data storage authority and may not alter any status pages, configuration files, or system settings. Supervisors may place user-created files in the proper location, review logs and add non-editable comments, and make limited configuration alterations. Administrators can make more sweeping configuration changes and assign users specific roles, while CDS editors enjoy root privileges. All accounts are password-controlled and manual entry of an appropriate password is necessary to move up to a higher privilege level. ICAS manuals promote an environment of access control by admonishing users to "always leave the workstation in the Normal User privilege level to prevent unauthorized users from tampering with the system." [73] Limited integrity of manually-entered data is maintained by a review system, which prevents data that has been reviewed from being altered by anyone with a lower privilege level, and rendering the data permanent once the data has been deemed to be official by the final reviewer. Limited auditing and accountability is attained by providing time-stamps of data that has been reviewed. Control of ICAS information flow has been achieved by enabling the system to only receive input from devices that it is directly connected to such as: a pre-existing external monitoring network that is interfaced with

ICAS; sensors that are installed on machinery and equipment, or manually inserted by a human operator directly into the ICAS workstation itself; or hand-held devices that can be connected directly to an ICAS workstation.

However, there are some access control problems as well. ICAS does not appear to have any restrictions on the composition or length of user-generated passwords, meaning that passwords could be dictionary words and thus easily exploitable. The ICAS installed on the U.S.S. Paul D. Foster appeared to require no password entry at all for the developer to access, indicating that the capability may exist within the system to bypass the password requirement entirely based on the configuration of the system. There is no information to indicate if ICAS passwords are stored in the clear or are encrypted. Although the ICAS manuals do make an attempt to promote good security awareness by warning users to execute their duties at the lowest possible privilege level, they also promote poor password practices by encouraging users to write down their passwords and store them in a safe place [37]. Information flow has also expanded beyond the restrictions originally placed on ICAS.

While two ICAS topologies—either directly connected to the ship's enterprise LAN or with access to the ship's LAN via a network switch—are intended to allow read-only observation of the data being monitored at a particular ICAS workstation, there is the possibility that ICAS data can be exposed to personnel who do not go through the same screening process of authorized users. Additionally, these administrative workstations may be kept in spaces that do not have the same physical access controls as the rest of the HM&E network. The incorporation of wireless networks within shipboard control systems, as embodied by the ICAS wireless vision illustrated in Figure 13, is yet another access control concern, especially given the aforementioned wireless security issues that are rampant within the federal government,.

Shipboard control system access control is an issue beyond ICAS. Vulnerability testing conducted against the U.S.S. Abraham Lincoln HM&E network revealed numerous security problems. External vulnerability scans exposed eleven discrepancies related to the Microsoft Windows operating system, two discrepancies with Hirschman Industrial Ethernet switches, four programmable logic controller flaws, and three

discrepancies with an Alcatel Omni switch. In addition, a review of the internal security configuration of Microsoft Windows host revealed seventeen flaws, including administrator account set to automatic logon; unrestricted registry access; no password required for user logon, lack of auditing; non-enforcement of strong passwords; and the caching of logon credentials [74]. Although many of these vulnerabilities were mitigated by the closed nature of the HM&E network, the capability of opening this network to the enterprise LAN (as allowed by ICAS) makes these vulnerabilities potentially exploitable by an attacker.

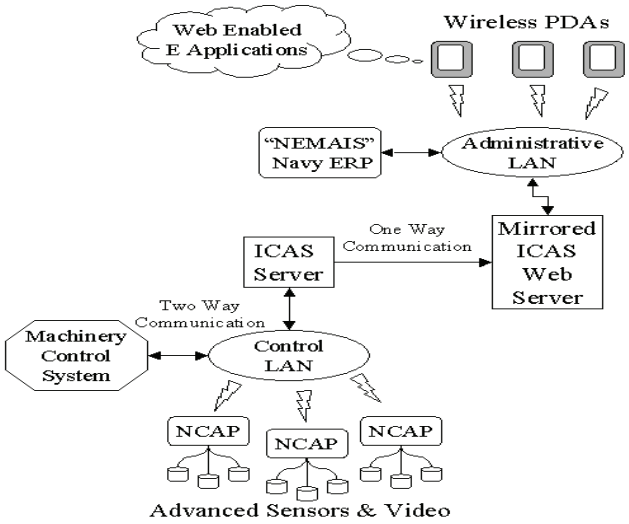

Figure 13. ICAS Incorporation of Wireless Networks (From [75]).

In addition, the ICAS logical boundary is growing. Previous versions of ICAS transferred information about ship systems to shore facilities via File Transfer Protocol (FTP), where analysts manually prepared written reports that were then sent back to the ships. However, newer versions of ICAS incorporate a remote monitoring capability that allows automatic downloading of ship data to a central server at Naval Surface Forces and Ship Systems Engineering Station (SSES) in Philadelphia, which automatically analyzes the data and generates the ship's performance appraisal report. It took sixteen days to get performance feedback to the ships using the old system; the new system gets appraisal reports back to the ship within twenty-four hours, allowing ship personnel to receive maintenance recommendations before warning conditions can degrade into

catastrophic failures [76]. Automated Common Diagrams (ACD) currently does not transmit information off the ship, but personnel intimately involved with this system envision that future iterations will be able to directly broadcast information to battlefield commanders, in order to provide an accurate picture of the battle-space by reporting on the material condition of assigned units, enabling leaders to allocate resources accordingly [34]. These technological innovations definitely have numerous operational benefits, but they also unquestionably place ship system data more vulnerable to exploitation.

3. Physical and Environmental Protection

Despite the demanding environment that Navy ships routinely operate in, shipboard control systems are offered physical protection that is well in excess of a normal SCADA system. Since the geographical area of shipboard control systems is completely self-contained within the hull, and the ship itself is built to withstand physical damage, these control systems are reasonably well defended against the physical threat posed by a hostile outsider. When they are pier-side at U.S.-controlled ports both within and outside the continental United States, Navy vessels are typically located at facilities that possess perimeter walls, continually guarded entry gates, and a mobile security force that regularly patrols the facility [74]. Vessels that are operating in foreign ports will employ extra security measures, such as anchoring ashore or posting extra guards pier-side, as a means of mitigating the threat posed from their proximity to unsecured facilities. Regardless of location, several security checkpoints must be passed in order to gain proximity to a pier-side vessel, to include roving vehicular and foot patrols on the pier, small craft patrols in the water, and stationary guards both on the pier and at the entry of the ship. Personnel manning these patrols are typically armed with firearms. Additional static defenses include defensive screens deployed in the water to prevent unobserved approach and fences partitioning off the adjacent dock space. Access to the facility requires an appropriately authorized identification, and access to the ship is restricted to ship's personnel, official guests, and personnel who possess a valid need to

come on board and who have been authorized by higher authority. While underway, the ship's mobility offers even tighter protection against the outsider threat, since access to the ship is obviously even more restricted.

In addition to the aforementioned staunch outsider physical protection, Navy control systems also have reasonable physical protection against the insider threat. Many shipboard compartments are controlled on an as-needed basis, and are accessible only to those personnel whose jobs legitimately require them to be granted access. These spaces include engineering, damage control, and computer network spaces, which is where the majority of the HM&E system would reside. Access to these spaces usually requires a key for a physical lock or the combination to a spin-dial or cyber lock, and many of these spaces are continually manned when the ship is underway. Sensitive compartments typically possess a list of authorized personnel, and guests to those compartments are usually escorted at all times. Additionally, despite the problems inherent within the DoD personal security clearance program, personnel that require access to these spaces for the performance of their jobs are often subjected to some form of screening process that often results in the granting of an interim or permanent formal security clearance, and are held to an established standard of personal reliability. These spaces are typically manned by authorized personnel around the clock while the vessel is underway, and secured after normal business hours when the vessel is in port.

Not only are Navy control systems afforded considerable physical protection against both outsider and insider threats, they are also typically operated in an inadequately-configured physical environment. Although many control system components are inescapably installed in places of extreme physical duress in order to directly manipulate the machinery they monitor, sensitive components of the network—such as servers, monitors, and workstations—are maintained in climate-controlled spaces where the air temperature and humidity are carefully regulated within specific tolerances. These components are often used in conjunction with an Uninterrupted Power Source (UPS) to protect against fluctuations in shipboard power, and can additionally be configured to operate off of shore power when pier-side. Navy shipboard spaces also

typically contain emergency firefighting equipment readily at hand as well as a large pool of personnel trained in emergency damage control, so the control systems vulnerability to fire is mitigated.

Naval vessels clearly provide significant physical and environmental protection to their control systems, but the very nature of their function can also place their systems at greater risk. Since naval vessels spend significant amounts of time in potentially hostile waters, the threat of physical attack is always present, and this provides a far greater potential for physical damage than what a CI control system might face. Logically, this potential for physical damage can, if translated to the reality of a combat situation, introduce control systems to the environmental hazard of fire, flooding, and exposure to toxic gasses. However, when contemplating security of control systems within the context of the overall function and mission of the vessel itself, the physical and environmental security enjoyed by shipboard control systems are about as good as one could expect.

4. State of Navy's HM&E Program

Yet another challenge to assessing the security of shipboard SCADA systems is the lack of a coherent structure in Navy HM&E. Equipment and machinery configurations vary among ship classes and even among ships of the same class, making a methodical and overarching security assessment approach impossible. Many ships use similar nomenclatures (such as MCS) to describe HM&E components that are actually fairly dissimilar to each other and which may incorporate different sensors, networking architecture and hardware. Each class ship maintains an HM&E system that encompasses several interfaced sensing and monitoring systems as well as various software applications, and these components can change from ship to ship. Many of these components offer similar functionality to the components used on other vessels, making them difficult to assess adequately. In addition, the sheer volume of HM&E components adds a further level of complexity to this problem. According to FY 2002 data, the Navy supports almost 150,000 unique HM&E components, with almost 19 percent of this equipment installed as a one-of-a-kind occurrence within the fleet [77].

The magnitude of HM&E components, coupled with the lack of a single HM&E model, makes it nearly impossible to make any concrete architecture recommendations.

Naval maintenance and procurement procedures contribute to this disjointed effort. Specific offices and individuals with the DoN exert control over their particular piece of the pie (such as ACD or ICAS), but there appears to be no single entity that oversees all HM&E systems Navy-wide. This leads to institutional tunnel vision, where there is a depth of knowledge about the individual HM&E components, but precious little understanding about the interaction of these components and how they coordinate to form a complete HM&E system. Interviews with members of the Navy's engineering community tend to support this observation; individuals were well-versed in the particular system they worked with, but demonstrated little comprehension of how that system related to the overall picture, and there were instances where the information they provided were later disproved by independent research of other sources.

Coherent information about the Navy shipboard HM&E effort is difficult to come by. Exhaustive Internet searches revealed high-level material about individual components, which was necessary to gain a basic understanding, but this information was wholly unsuitable for conducting an exacting analysis. Personalized contacts provided operating manuals and other useful sources that allowed a closer examination of the systems, but these sources were still lacking the required technical detail, and the piecemeal extraction of such details from the contacts was a laborious process. In many cases the contacts either could not, or would not, reveal the desired information. This problem is exacerbated by the proprietary nature of the applications involved

The multiple problems of control system vulnerability, both in civilian industry and within the military, depicts an infrastructure whose security foundation is shaky at best, at a time when the potential threats to that infrastructure seem to be multiplying. Adding yet another reason for concern is the fact that the majority of control system components are manufactured in foreign countries, providing a potential opportunity for hostile insertion of exploits specifically designed to take advantage of a well-documented weakness. As of this writing, there has not been a single magic bullet designed to bring the security problem to a manageable level, and the complexity of the problem is such

that this cookie-cutter solution may never be discovered. However, there have been some attempts to systematically address this issue, and a general examination of some of these methods for correcting, or at least mitigating, the vulnerabilities of control systems will be the subject of Chapter VII.

VII. IMPROVING THE SECURITY OF CONTROL SYSTEMS

Despite the obvious need to harden control systems, the critical infrastructure industries appear to have made little progress in addressing the vulnerabilities of their systems. There has been enormous attention paid to ensuring that control systems operate in a reliable and optimum manner under normal circumstances, but there has not been a comparative effort made to determine how those control systems respond to "extreme events, contingencies, massive or cascading failures, or malicious attacks." [78] Evidence of the lack of progress in control system security is demonstrated by comparing past vulnerability assessments with more recent evaluations. In 1997, the National Security Telecommunications Advisory Committee (NSTAC) Information Assurance Task Force conducted a cyber risk assessment of the electric power industry. The results of this assessment are comparatively displayed with the results of similar 2002 assessments conducted by the the Institute of Electrical and Electronics Engineers (IEEE) in Table 5.

Table 5. Power Grid Vulnerabilities (After [78]).

Documented SCADA Vulnerability	1997 NSTAC	2002 IEEE
Weak passwords used	yes	yes
Default passwords not changed	yes	yes
Passwords posted visibly	yes	yes
Shared logins	yes	yes
Inconsistent or non-existent warning banners	yes	yes
Personnel unaware of hacking threat	yes	yes
Unsecured modem access	yes	yes
IT network interconnectivity	yes	yes
Non-existent or inadequate intrusion detection	yes	yes
Non-existent security policy	yes	yes
Internet connectivity	non-existant	yes
Wireless networks	non-existant	yes
Commercialization of utility telecommunications	non-existant	yes

These results clearly show that the security problem for control systems is increasing rather than diminishing. All of the vulnerabilities found in 1997 were rediscovered in 2002, and additional vulnerabilities, which are the result of emerging technology and enterprise practices, have emerged as well [78].

Although many, if not most, critical infrastructure industries do not appear to be improving their defensive posture, this is not to say that the subject has been stagnant. Computer security professionals have been focusing considerable attention on the matter, and their efforts have produced some promising possibilities. The various peculiarities, and unique challenges, of control systems may make a completely secure system impossible to achieve. However, the research that has been done has yielded guidance and innovations whose implementation could make the security problem more manageable.

The proper approach is to initiate a defense-in-depth strategy. This is a combination of technical and non-technical defenses that are designed to provide overlapping, layered protection against hostile intrusions into the system. Technical defenses are those security solutions that can be implemented in computer hardware and/or software, whereas non-technical defenses are security measures that are implemented independent of the hardware or software that is used, such as security policies and personnel screening requirements. The concept is to ensure that security is not focused solely in one area, but is instead applied across many different avenues, with the various components providing support to the others. This eliminates weak spots and improves the overall security of the system. A strategy for improving the security of control systems is presented in the following sections.

A. EVALUATION AND CERTIFICATION OF CONTROL SYSTEMS

There are many technologies that are useful in reducing the vulnerabilities of a system or a network. Research is currently underway to determine if, and how, these technologies may be adapted to the particular environment of a control system, and some of these will be discussed later. However, these solutions are merely one aspect of system protection, and do not by themselves constitute adequate protection. For

example, firewalls are used to regulate traffic flow into and out of a system, and intrusion detection systems (IDS) are used to detect unauthorized intrusions into a system, but these products cannot completely overcome inherent weaknesses in the system itself.

The solution to this problem is to have a system where security is "baked-in" and not "brushed-on"—in other words, where security is not added as an afterthought, but is included as part of the design and developmental process. Evaluation and certification of the control system is one means of ensuring this. Security in an IT system can be defined as the degree to which the information in the system is protected from unauthorized disclosure, modification, or loss of use by countering threats to that information arising from human or systems-generated activities, malicious or otherwise [79]. In order to make a claim about the capability of a system to protect the information it contains, there must be some way to express the level of security that system, and there must be some way for system users to be confident that the system offers the correct level of protection. This process is known as evaluation and certification, and the International Common Criteria for Information Technology Security Evaluation, also known simply as the Common Criteria (CC), is one way to implement this process.

1. Common Criteria (CC)

Recognized as Standard 15408 of the International Standards Organization (ISO), the CC was designed as a means of defining, expressing, and verifying the security requirements of an IT product or system. It defines 7 different numbered classifications of security assurance, known as Evaluation Assurance Levels (EAL), each providing a particular level of confidence that the system or product meets its security objectives, with increasingly stringent testing and verification. Common Criteria ensures that computer security specification, implementation and evaluation has been rigorously performed following a standardized methodology.

The CC allows developers to construct their product and prepare it for third-party evaluation by defining the security requirements of the product. It also assists evaluators by describing a set of general actions that must be conducted, and the security functions

that must be tested, while performing the evaluation. Consumers can then use these evaluations to determine if a product or system meets their specific security needs.

The product that is examined by the CC can be the entirety of an IT product, a part of an IT product, or even a collection of IT products. Examples of a product include a software application, and operating system, a database application, a LAN, or combinations of these. In other words, it is "a collection of software, firmware and/or hardware accompanied by guidance." [80]

Since products can often be established in many different configurations, each of which has unique operating characteristics, a CC evaluation is only good for a specific configuration, which is known as the Target of Evaluation (TOE). Evaluation is an assessment conducted against defined criteria and is used to validate claims made against the TOE. Simplistically, the CC does this by means of either a Protection Profile (PP) or a Security Target (ST).

The PP is an implementation-independent set of security requirements for a broad category of TOEs. It is typically a statement of common security needs defined by a user community, a regulatory entity, or a group of developers, and is used to serve as a template for a Security Target. It is therefore typically used as part of a requirement specification for a specific consumer or group of consumers, or as part of a regulation from a specific regulatory entity, who will only allow a specific type of IT to be used if it meets the PP. It can also be used to define a baseline determined by a group of IT developers, who then agree that all IT that they produce of this type will meet this baseline. The PP can then be used by vendors to create STs to meet security requirements and have their products evaluated by a third party. It is not meant to be either a detailed or complete specification, and unlike the ST, it is not intended to refer to a single product [80].

The ST is an implementation-specific set of security requirements for a specific TOE, often using a Protection Profile as a template. Before the product is evaluated, the ST serves as a means of identifying what precisely is to be evaluated, and defines the scope of the evaluation and the specific security objectives of the TOE. Once the

evaluation is completed, the ST identifies what has been evaluated, and describes the exact security properties in such a way that consumers can have a clear understanding of what the TOE offers. It is not intended to be either a detailed or complete specification [80].

After a product has been evaluated, it can then undergo the process of certification. Certification is the independent inspection of the evaluation results which can then lead to a certificate or approval, thereby ensuring greater consistency in the application of various security criteria [80].

2. Application of the Common Criteria to Control Systems

Because it is designed to provide a rigorous assurance that a product meets specific security objectives, work has been done to apply the CC to the development of secure control systems. This effort was prompted by the ISO TC 57 Ad Hoc Working Group 6 initial report on data and communication security, released in September 1999. This report focused the utility industry to move away from a threat-based security approach and towards a consequence perspective for security assessment and asset identification, and also directed the utilization of Common Criteria protection profiles to develop a SCADA security standard [45]. Some of the protection profiles that have been developed as a result of this are discussed below

a. Tele-Control Application Service Element2 Protocol

In 2000, Sandia National Laboratories (SNL) released a protection profile for the Tele-control Application Service Element.2 (TASE.2) protocol. Also known as the Inter-Control Center Communications Protocol (ICCP), TASE.2 is widely used to exchange information between SCADA control centers. Because ICCP is used by utility industries around the world, and because the security of this protocol is fundamental to the security of communications and control within the SCADA network, there is a high priority to establish a secure standard for it. This SNL report represents the first PP for a SCADA protocol and is the first SCADA security specification based on industry standards [45].

The TASE.2 PP establishes the security environment of the TOE by making assumptions about the security environment and describing security policy issues. Security threats are identified, and security objectives that map to the threats are established. The PP then describes security functional requirements that will address the needs described by the security objectives [81].

b. ICS System Protection Profile

Decisive Analysis has released a System Protection Profile (SPP) for Industrial Control Systems (ICS). An SPP is designed to be a protection profile that captures the common subset of security requirements that are applicable to all ICS applications, and, unlike an ordinary PP, can include factors (such as security training and risk assessment) that are beyond the control of a vendor but which are still essential for a secure environment. The ICS SPP "includes requirements for operating policies and procedures, requirements for information technology based system components, requirements for interfaces and interoperability between system components, and requirements for the physical environment and protection of the system." [82] It can be used as the basis for preparing a System Security Target (SST) for a specific ICS, or as the basis for a more detailed SPP for a sub-class of ICS such as a SCADA. This concept is illustrated in Figure 14.

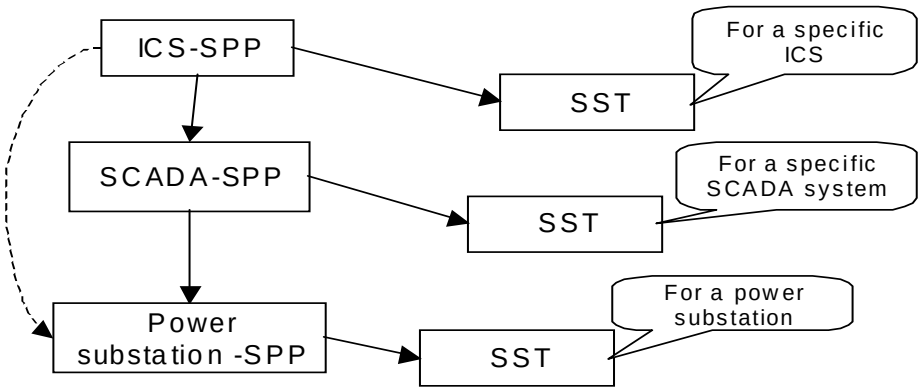

Figure 14. Relationship between SPP-ICS and other potential SPPs and STTs (From [82]).

The ICS SPP establishes the security environment by stating security usage assumptions, describing security threats and vulnerabilities, listing assets within the scope of the SPP, and detailing organizational security policies. The SPP then identifies risk categories and maps the risk categories to the appropriate threats, vulnerabilities, and assets. The security objectives and functional security requirements are then described. Security assurance requirements are then discussed in order to confirm that the system achieves an acceptable residual level of risk. These organizational sections of the ICS SPP are intended to flow naturally from one to the other, as depicted in Figure 15.

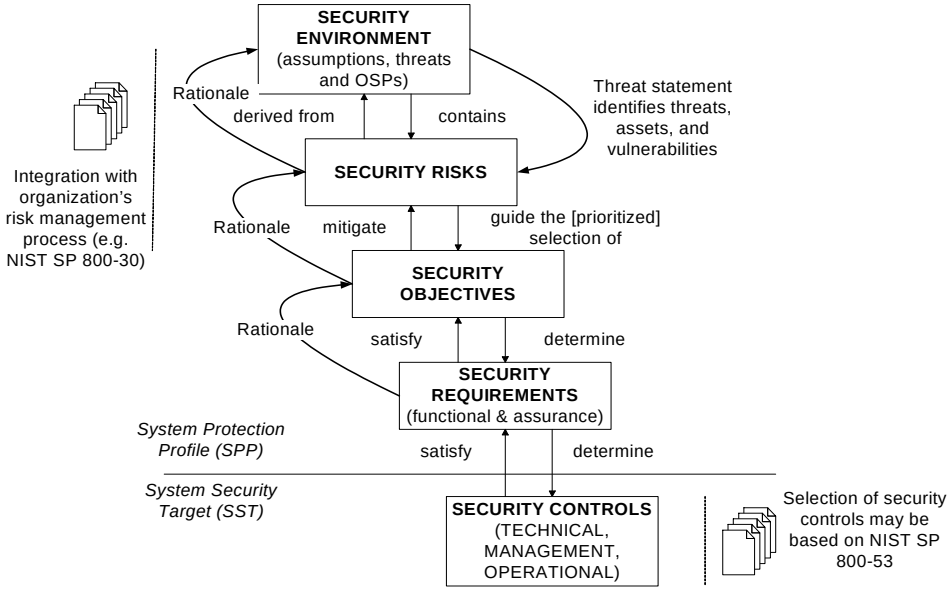

Figure 15. SPP-ICS Structure (From [82]).

Decisive Analysis has also released a SPP that is specifically designed for critical infrastructure control systems, using the ICS SPP as a starting point for this document. Organizationally and structurally, it is almost identical to the ICS SPP, with the main difference being that its written goal is to provide a written high-level set of security requirements for a generic critical infrastructure ICS [83].

c. ICS Control Station Protection Profile

(3) Digital Bond has developed its own SCADA Protection Profile. This PP is designed to provide a set of functional requirements for an ICS control station, including the control servers, historical servers (to maintain historical data), HMI, and the associated network. The scope of the PP can include back-up control stations and may include control stations that are stationed at remote sites, but it specifically excludes RTUs, PLCs, and other field devices. It also excludes communications to and from these field devices as well. The PP boundary is shown below.

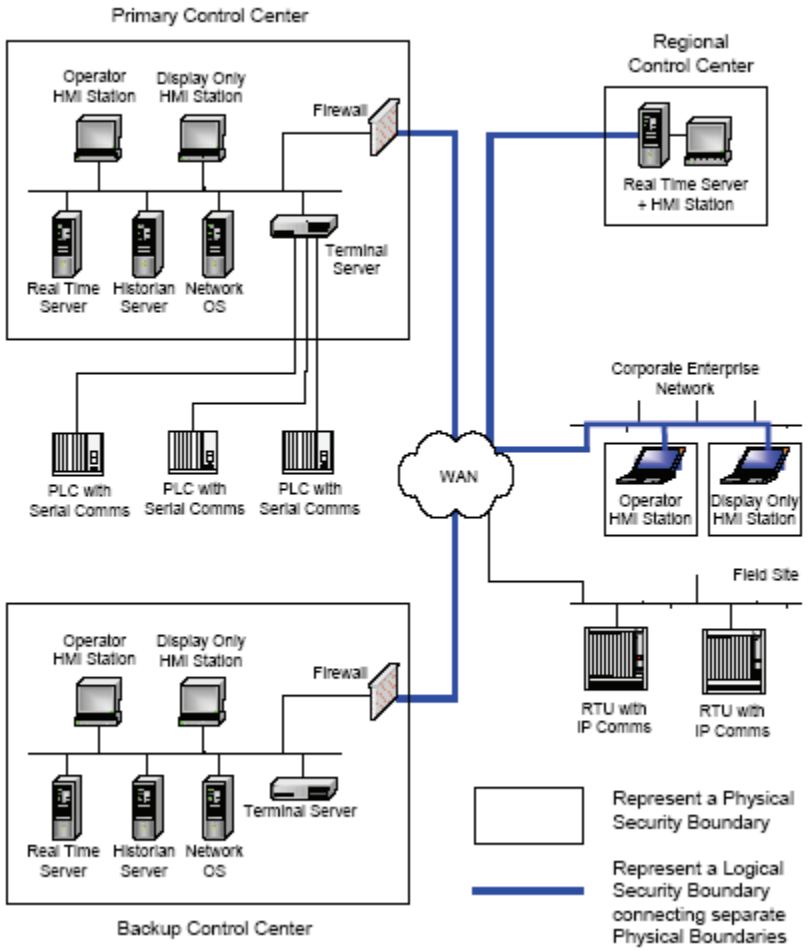

Figure 16. Cyber Security TOE and Security Perimeters for Control Center PP (From [83]).

There are a variety of reasons the Control Center PP excludes field devices from its scope. First of all, most of the solutions to control system vulnerabilities appear to be part of the control center, so it makes sense to focus attention on this portion of the system. Furthermore, many vendors have developed control centers that implement industry standard security protocols, and the shortest path to getting a Common Criteria certified product in the near future may be by drafting a PP for an area that has already made great security strides. Field devices are still highly proprietary and it may be several years before their security issues are addressed, and as a result they are treated as untrusted subjects by the Control Center PP. However, Digital Bond hopes that when standards for field devices are developed and a Field Device PP is drafted, this could lead to a completely certified ICS [84].

The organization of the Control Center PP is similar to the protection profiles previously discussed. The security environment is explored by describing security assumptions and threats. Security objectives are then explained, and security functional requirements are documented. The PP then maps the security objectives to the threats the objectives are designed to counter. The objectives are then mapped to the security functions, and a reverse mapping of the security functions to the objectives is also provided.

3. Alternatives to the Common Criteria

The Common Criteria has come under fire from representatives in the security and academic fields. The CC process has been accused of being prohibitively expensive and provides no guarantee that the customer is getting a product with improved security. The lower EALs, where most products are evaluated, only require evaluation of the development process and documentation, rather than the software itself, due in large part to the preponderance of proprietary code that the CC is applied to. This failure to mandate code reviews prevents an examiner from searching for programming bugs and results in a closed evaluation system that cannot be replicated by different laboratories. In addition, the Common Criteria focuses on the product design and documentation but does not examine the product in its operating environment, and can give the buyer

confidence in the specification, but not the implementation [85]. Furthermore, the evaluation process is cumbersome and time-consuming, resulting in many products being evaluated as they near obsolescence, and forcing the customer to decide between choosing an out-of-date product with a valid security evaluation, or a newer product that has not been evaluated.

Because of these shortfalls, assurance alternatives that may be more time-efficient, less costly, or comprised of different evaluation methodologies, may be pursued in place of the Common Criteria. These alternatives may follow the same product-based paradigm as the Common Criteria, such is the CESG Claims Tested Mark (CCTM), which targets the lower CC EALs and is designed to provide a cost-effective assurance scheme with a reasonable timeliness factor. However, a developmental assurance model might be utilized instead. Examples of this sort of model include the System Security Engineering Capability Maturity Model (SSE-CMM) and the Capability Maturity Model Integration (CMMI) both of which attempt to provide assurance by making a judgment of the maturity of the process involved in performing the security activity, rather than judging how the activity is accomplished.

Regardless of the method, it is important to subject a control system to some sort of evaluation and certification process. Regardless of the flaws of this process, it can allow for the declaration of how well the product meets specifically articulated security requirements, as well as some form of impartial validation of this claim. This is important to providing a degree of assurance that the risk to the system is reduced.

B. INCORPORATION OF CYBER SECURITY STANDARDS

Various elements and components of the critical infrastructure industry are in the process of developing guidelines and security standards for use within their respective infrastructure. The incorporation of these cyber security standards is an important step in improving the security of these different infrastructures, and can accomplish the dual purpose of heightening awareness of control system security vulnerabilities, and providing a more stringent defense against intrusions. A comparative analysis of these security standards reveals a wide range of security issues that are addressed, as well as

varying degrees of detail. Some provide fairly broad-brush guidance on a wide range of security subjects, while others offer more specific direction, but all of them can be useful for the particular industry in question.

1. ISO/IEC 17799

The International Standards Organization/International Electrotechnical Commission (ISO/IEC) 17799, also known as "Code of Practice for Information Security Management," is a high-level, detailed, general purpose security standard. It is organized into ten sections, covering such topics as business planning; access control; system development and maintenance; physical, personnel, and environmental security; security organization and policy; and computer and network management. It was not written specifically for control systems, but many critical infrastructure industries use it as a starting point when developing their own security standards and it serves as a good basic building block for constructing a security standard and tailoring it to a particular environment.

2. North American Electric Reliability Council (NERC)

In response to Presidential Decision Directive 63, the U.S. Department of Energy designated the North American Electric Reliability Council (NERC) as the coordinator for the Electricity Sector of the nation's critical energy infrastructure. This designation makes NERC responsible for identifying weaknesses in the electrical power industry, devising ways to reduce these vulnerabilities, construct a system that identifies attacks and allows warnings of attacks to be disseminated, and assist in reconstituting minimum electrical services in the aftermath of an attack [86]. As the watchdog for the electrical sector, NERC has issued several documents to fulfill its responsibilities in this area, two of which are discussed below.

a. NERC Security Guidelines for the Electrical Sector

NERC published these guidelines in 2002 as a means to support the electrical industry's attempts to re-evaluate existing plans and procedures currently in place to deal with attacks against this critical infrastructure component. The guidelines

are advisory in nature and are intended to apply only to critical operating assets, which each company being free to make their own determination as to those facilities and functions that are actually critical. This document describes nine different security guidelines, including vulnerability and risk assessment, threat response capability, physical and cyber security, and the protection of potentially sensitive information.

b. NERC/CIP

In August 2003, NERC issued a document known as NERC 1200, which was intended to be a temporary standard that was designed to establish minimum-security standards for the electrical industry, in order to lower the risk of critical asset compromise. This temporary standard was in effect while a permanent standard was being written. The first draft of this permanent standard was released in September 2004, with subsequent drafts being released in January 2005 and May 2005. The current incarnation of this document is known as the North American Electric Reliability Counsel Critical Infrastructure Protection (NERC/CIP). NERC/CIP details eight different standards, each of which describes a particular security area. These standards are listed below:

(1) Critical assets
(2) Security management controls
(3) Personnel and training
(4) Electronic security
(5) Physical security
(6) Systems security management
(7) Incident reporting and response planning
(8) Recovery plans for critical cyber assets

The NERC/CIP serves the same basic purpose of the NERC Security Guidelines for the Electrical Sector—to provide some measure of cyber security to reduce the vulnerabilities of the electrical industry from attack. However, it is far more detailed and far more directive in nature. Each of the eight standards within the NERC/CIP describes compliance requirements that must be met in order for that

particular section to be satisfied, and each section standard explicitly states measures that must be taken that will be used to determine compliance. Critics of the NERC/CIP believe that the standards are not rigorous enough and, hence, will lead to ambiguous implementations that do not reach their full security potential, but the very lack of rigor could make for a more rapid consensus among the various electrical companies, as well as a far easier implementation process, and compliance with this standard should, on balance, provide a considerably improved security posture than is currently the case [87].

3. American Petroleum Institute (API) Standard 1164

The API represents 400 members involved in the nation's oil and natural gas industry. In an effort to address the security considerations of this component of the critical infrastructure, it released API Standard 1164. API 1164 targets small to medium-sized companies, and is intended to improve the security of pipeline SCADA systems by describing how to identify and analyze SCADA vulnerabilities, providing a list of practices to harden the core architecture, and highlighting examples of the best current practices in the industry [88].

API 1164 is simplistic in nature, and thus easier to implement than a more precise standard would be. It addresses such topics as access control, communications, information distribution, physical security, network design, and security management. The standard includes two helpful appendices that provide a significant amount of detail to the overall document. Appendix A is a security checklist designed to be used as a guide when reviewing the security of SCADA systems, while Appendix B is a sample control system security plan. Although the standard lacks technical rigor, it serves as a useful starting point for improving the security of a petroleum or natural gas utility.

4. American Gas Association (AGA) Report Number 12

The AGA represents 192 utility companies that deliver roughly 83 percent of all delivered natural gas to homes businesses, and industries. In concert with the Gas Technology Institute, and in coordination with representatives of the gas, water, and electrical industries, as well as manufacturers, SCADA operators, and government

agencies, the AGA has produced AGA Report Number 12. AGA 12 was conceived as a four-part series of documents that focus on securing the communications of SCADA systems, with the goal of providing communications that are capable of being authenticated by valid users and can provide a high-assurance of being unaltered by potential attackers [88].

The most recent draft of the AGA-12, Part 1, is organized into five sections and several appendices. Section 1 is an overview of the standard. Section 2 describes SCADA system vulnerabilities and possible means of compromise as well as cost impacts of implementing the standard. Section 3 provides guidance on how to define security goals, understand vulnerabilities and threats, and determine the best course of action. Section 4 lists various system compliance requirements, cryptographic performance requirements, cryptographic system design goals, and cryptographic module components. Section 5 serves as a technical reference. The detailed annexes include substantial background information, covering such topics as SCADA fundamentals, cryptography fundamentals, security practice fundamentals, and challenges of applying cryptography to SCADA communications.

AGA planned to issue additional documents in AGA-12 series, including standards for SCADA embedded system cryptography and protection of IP-based SCADA networks. However, these other reports were terminated due to lack of funding, and no public drafts of these reports have been discovered. However, it is hoped that the work done on this report can pave the way for the eventual development of a standard will significantly enhance the overall security of SCADA communications in general.

5. Chemical Industry Data Exchange (CIDX)

The chemical industry, like most other components of the critical infrastructure, is addressing the security of the SCADA systems under its control. The Chemical Industry Data Exchange (CIDX) is the standards body that has been engaged to develop security practices and guidelines within the chemical industry, and has published a report titled “Guidance for Addressing Cybersecurity in the Chemical Sector” in support of that mission. This standard details nineteen key elements that are critical to the protection of

the chemical infrastructure, including access control; risk management and implantation; incident planning and response; and organizational, physical, personal, and environmental security. The elements are described in terms of how they are applicable to cyber security and how to employ it. The guidance document is similar to the NERC/CIP in that it is a high-level standard that does not impose rigid, specific restrictions, but whose application will still have a measurable positive affect on the security posture of its target industry [89].

6. Department of Energy 21 Steps

The U.S Department of Energy, in conjunction with the President's Critical Infrastructure Board, released a SCADA security guidance document entitled "21 Steps to Improve Cyber Security of SCADA Networks." It is designed to briefly outline recommended steps that provide a common-sense approach to increasing control system security across all industries. Steps 1 through 11 describe specific actions that can be undertaken to improve the security of the SCADA system itself, such as the identification and hardening of all connections to the SCADA network; performing physical security surveys, incident monitoring, and technical audits; and implementing the inherent security features that are provided by device and system vendors. Steps 12 through 21, on the other hand, focus on the essential underlying security management policies and processes; such as clearly identifying cyber security roles, responsibilities, and requirements; establishing effective risk-management, configuration management, and response recovery plans that are reviewed on a periodic basis; and ensuring that minimal security expectations and security policies are written and disseminated to all personnel. Although this is not a security standard *per se*, it serves as a good high-level path that can serve as a blueprint for an overall improved security position [90].

7. NIST Special Publication 800-53 Annex I

The National Institute of Standards and Technology (NIST) recognizes that control systems have unique considerations when compared to normal information systems and thus require specialized security attention, even though the inclusion of

commercially-used software and hardware has narrowed that divide somewhat. NIST Special Publication 800-53 outlines recommended security controls for federal information systems, and Appendix I focuses specifically on control systems. This Appendix provides tailoring guidance, security control enhancements, supplements to the security control baselines, and general supplemental guidance that can all be applied to improving the security of control systems [67].

8. SCADA and Control Systems Procurement Project

Because critical infrastructure security has gained heightened awareness in recent years, a multi-agency initiative was spawned to improve the nation's control systems cyber security posture. This joint private and public sector initiative was assembled by the Department of Homeland Security National Cyber Security Division, Idaho National Laboratory, the Chief Information Security Officer (CISO) of New York State, and the SANS Institute. The project, which is populated by 242 international public and private sector entities, is designed to allow "private and public asset owners and regulators to come together and adopt procurement language that will help ensure that security is integrated into control systems." [91]

Adhering to industry standards and following established industry guidelines can improve the security of a control system. These measures allow measurable criteria to be created that can provide the blueprint to more secure systems throughout the industry , thereby shepherding control system development towards a more secure pattern.

C. ADDRESSING CONTROL SYSTEM NETWORK PROBLEMS

Many of the security problems inherent in control systems are due to issues involving the transfer of information to and from master control stations to remote stations. These problems include interconnectivity of the control system network to other networks, transmission of control system information via shared communications channels, control system message restrictions that hamper corrective measures such as authentication and encryption, insecure remote access into the network, and utilization of

standardized communications protocols that are ill suited to a secure control system network. Performing the following steps will go a long way towards reducing the vulnerabilities of control system networks and will greatly improve the overall security of the system.

1. Harden the Control System Networks

In this age of computer network growth, many critical infrastructure entities are using common TCP-IP protocols as the communications standards for their control systems. Because these protocols are the backbone for Internet communications, many of these entities have connected their SCADA networks to their enterprise LANs. While this allows for improved executive efficiency and heightened dissemination of control system information, it also drastically increases the vulnerability of control system networks to potential threats. Business LANs are commonly connected to the Internet, and exploitation of the enterprise LAN by an attacker could lead to a similar compromise of the control system network. An additional danger is the likelihood for backdoors into the system by contractor personnel, which can be easily exploited by malicious intruders.

There are several steps that can be taken to improve the defense posture of the control system network. The network must be thoroughly mapped in such a way that all elements of the network, and all possible access points into the system, can be identified. Unnecessary access points and backdoors should be eliminated, and the control system network should be isolated as much as possible from other networks. Control system messages should, in no case, ever share the same network paths as other computer traffic. Remote access into the network should be severely restricted, and should employ effective authentication techniques, such as strong passwords and individual user accounts. Finally, the remote elements of the network should have some measure of physical protection against unauthorized access, and should employ some measure of strong authentication (such as a password and a token, for example) to resist the entrance of malicious individuals who manage to gain physical control of the remote device.

It is important to ensure some measure of partition between control system network and the corporate network. The easiest method of doing this is to make the two systems complete distinct and separate. This will provide significant assurance that only authorized control system users are accessing the control system network. However, it may not be practical to implement this solution, so the following section will address the reality of co-mingling the corporate and control system networks, and ways to mitigate the dangers inherent in this situation.

2. Make Effective Use of Perimeter Security Tools

An important aspect of securing the network, which was implied in the previous section, but which will be specifically discussed here, is the establishment of perimeter security tools. Businesses will, in many cases, be reluctant to lose the convenience afforded by interconnecting the control system network with the enterprise LAN, and it may not be possible to eliminate all vendor access into the SCADA system. It is therefore important that the business LAN, as wells the control system network itself, makes effective use of appropriate security perimeter tools.

a. Intrusion Detection Systems (IDS)

Intrusion detection systems are designed to detect unauthorized access into the computer network. An IDS is either host-based or network-based. A host-based IDS (HIDS) is resident in a computer host and analyzes activity within that host, matching patterns of behavior with pre-loaded "signatures"— characteristics that match a hacking exploit—that match suspicious activity. A network-based IDS (NIDS) does essentially the same thing, except that it performs this activity for an entire network rather than a single machine. IDSs are commonly used in conjunction with other security tools (explained below) to form the defensive perimeter of the system.

b. Firewalls

A firewall is a mechanism that is used to monitor the traffic that flows into, through, and out of a computer network. It accomplishes this task by comparing the traffic packets against guidelines that embody a specific security policy, and only passing

traffic that meets the appropriate criteria. Firewalls can either be completely separate hardware components, a completely host-based software application, or a combination hardware/software mechanism. Network firewalls are typically of the hardware or hardware/software variety, and these are the devices most appropriate for use on a control system network, although host-based mechanisms can also be included.

Firewalls can perform additional functions in addition to the basic function of controlling traffic routing. Firewalls can act as a first-level IDS by logging those packets that are denied access, reporting unusual problems with the traffic, or by recognizing potentially troublesome packets. Some firewalls can also act as a front-line anti-virus mechanism, by recognizing traffic packets with virus characteristics and blocking this traffic from entering the network. Firewalls can also provide authentication services, VPN gateway services, and network address translation services [92].

The goal of the firewall is to minimize unauthorized access of traffic onto the control system network, and there are general guidelines that need to be followed, and which the firewall needs to enforce, in order to realize this objective. First, there should be no direct connections from the Internet to the control system network, and vice versa. This is to prevent inbound traffic from congesting the network (and in extreme cases, initiating DoS attacks) and to prevent the same issue from occurring with outbound traffic. Second, there should restricted access from the enterprise network to the control system network. Both networks should be physically and logically isolated. Yet another guideline is to support authorized remote access, in the event that support is absolutely required, needs to be done in a secure fashion. Finally, there needs to be well-defined rules defining the type of traffic allowed on the network.

There are a variety of firewall architectures that could be deployed on a control system network. The configurations vary in cost, complexity and effectiveness, and each configuration has its own particular weaknesses and strengths. The selection of any particular architecture will require some sort of trade-off in terms of scalability, manageability, and degree of security provided. Loosely speaking, these architectures can be broken into three general categories: those that achieve separation using non-firewall devices such as dual-homed workstations, bridges, and routers; those that

incorporate a two-zone firewall design that does not utilize a demilitarized zone (DMZ); and three-zone firewall designs that do incorporate a DMZ. Of these categories, the use of a DMZ generally provides the best combination of security, scalability, and manageability [92].

The effectiveness of a firewall depends on the rules that dictate how it controls the traffic it monitors. It is vital that special care is taken to correctly establish the rules set of the firewall. Incorrectly-configured firewalls will not only fail to properly shield the system, but will also, merely because the firewall is deployed, give IT personnel a false sense of assurance about the protection it provides. Suggested guidelines to follow when configuring a firewall are shown below in Table 6.

Table 6. Recommended Firewall Configuration Guidelines (After [92]).

Num	Guideline
1	The base rule set should be Deny All, Permit None.
2	Connections between control system network and any external network should only be enabled on a case-by-case basis, with documented justification regarding why the information flow is allowed.
3	All "permit" rules should be both IP address and TCP/UDP port specific, and stateful if appropriate.
4	All rules shall restrict traffic to specific IP address or range of addresses.
5	Any non-IP protocol should be dropped, since communication on control system networks is typically IP-based.
6	Prevent traffic from transiting directly from the control system network to the enterprise network. All traffic should terminate in the DMZ.
7	Any protocol allowed between the control system network and DMZ is explicitly NOT allowed between the DMZ and enterprise networks (and vice-versa)
8	All outbound traffic from the control system network to the enterprise network should be source and destination restricted by service and port using static firewall rules
9	Allow outbound packets from the control system or DMZ only if those packets have a correct source IP address assigned to the control system or DMZ devices;
10	Control system devices should not be allowed to access the Internet. control system networks shall not be directly connected to the Internet, even if protected via a firewall.
11	All firewall management traffic be either via a separate, secured management network or over an encrypted network with two-factor authentication. Traffic should also be restricted by IP address to specific management stations.

Unfortunately, the protection that firewalls provide control system networks is somewhat limited. Firewalls are designed to deal with Internet protocols, and these firewalls have no knowledge of control system-specific protocols and services, and the rules set of a firewall offers no protection against an attack against a control system-specific (and inherently insecure) protocol such as MODBUS. Therefore, while "the current systems are excellent against script-kiddie hackers and other novices that use exploits easily available on the Internet; they are not adequate to detect attacks by a SCADA cyber terrorist, disgruntled insider, or skilled hacker with knowledge of SCADA systems." [83] Firewalls that have knowledge of control system processes and protocols need to be developed to address this vulnerability.

c. Combination Strategies

The security perimeter of a SCADA system is most effective when a combination of tools is used. In order to envision the concept of a security perimeter, consider the physical analogy of a secure building. The building will have locks on the doors and windows, and probably a fence around it as well, to prevent illegal entry into the premises. Physical monitoring systems, such as cameras and motion detectors, are often used to identify breaches and enable a quick response. The locks, fences, cameras, and monitors form the security perimeter for the building [93].

Dale Peterson of Digital Bond uses this parallel to define the security paradigm of a control system network. The firewall is designed to prevent unauthorized access, fulfilling the same function as the locked windows, doors, and fence. Intrusion detection systems perform the monitoring and detection functions. Additional tools, such as the collection of host log entries and the continued analysis and evaluation of the information gathered from NIDS, HIDS, audit logs, and other sources, can assist the IDS for maximum effectiveness by revealing important information about activity on the system, such as failed and successful intrusion attempts, processes initiated by the intruder, or escalation of privileges, and so on. This can all help determine if an attack has occurred or is in progress, and initiate a rapid response to it.

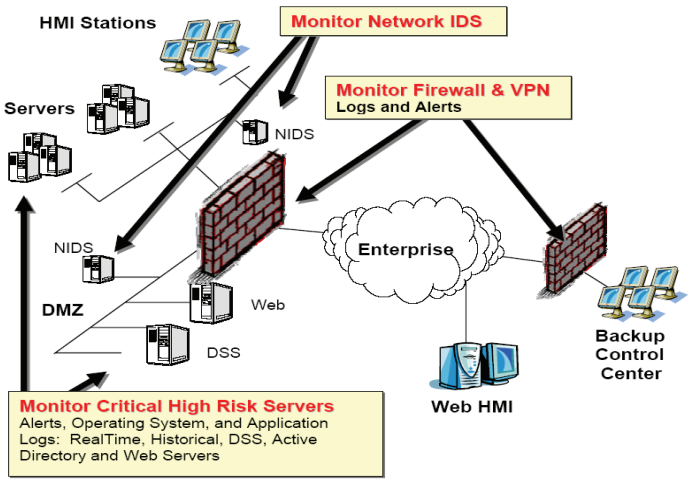

Figure 17. Cyber security monitoring (From [93]).

As is seen in Figure 17, firewalls form the outer perimeter of the network by restricting traffic to and from the control system network and the enterprise LAN, and their audit logs can be analyzed to detect access attempts into the control system network via the enterprise LAN. Network Intrusion Detection Systems are stationed in the control system LAN as well as within a DMZ that commonly contains systems such as web servers and historical servers that have a legitimate need to be accessed from the enterprise LAN. Monitoring of all the logs is conducted to identify security events and accurately classify the occurrence of an attack, as well as the severity of an attack once it is identified [93]. This configuration provides a layered defense perimeter against an attack against the system. Some examples of the benefits of this configuration are illustrated in Table 7.

Table 7. Benefits of Defense in Depth (After [93]).

Description of Attack	Results of Attack	Benefit of Defense Tools
An attack is launched against the CONTROL SYSTEM network via the enterprise LAN	Attack is stopped by an effective firewall with a well-constricted rules set	Monitoring of firewall logs can serve as an early-warning of a possible attack and can either identify a disgruntled insider or a vulnerability that is exploited by a hacker from the outside.
An attack from the enterprise LAN gets by the firewall and is targeted for the DMZ	Attack will be detected by the firewall logs, the NIDS, and the logs of the targeted DMZ machine.	Analysis of this information would confirm the existence of the attack, as well as revealing whether or not the attack was successful.
An attack is launched against the CONTROL SYSTEM network itself	Attack will be identified by the NIDS	Examination of the audit logs of the stations within the CONTROL SYSTEM network could aid in the determination of the success or failure of an attack
Disgruntled insiders and outside hackers that gain access into the enterprise LAN may perform a network scan to identify vulnerabilities	NIDS and firewall audit logs can detect the scanning attempts.	NIDS and firewall audit logs can possibly be used to prevent the attack

3. Protect Transmitted Control System Communications

A major problem with control system communications is that they are extremely susceptible to exploitation. Many control systems use shared channels to transmit their data, and this information is commonly passed in plain text, thereby affording an attacker not only ease of collection of control system data, but ease of interpretation as well. In addition, while most control system protocols utilize some form of Cyclic Redundancy Check (CRC) to detect errors caused by noise, there is no known control system protocol that ensures integrity against a malicious entity [94]. Common assumptions about control system communications, as well as the truth about the vulnerability that the assumption masks, are listed in Table 8. Examination of this information shows that not only is the security of control system message traffic at considerable risk, but that there is also an apparent lack of concern about these inherent vulnerabilities. Protecting control system communications would therefore significantly increase the security of the system.

Table 8. Realities of the vulnerabilities (After [95]).

ASSUMPTION	REALITY
We use leased lines, so nobody has access to our communications.	It's easy to tap these lines. The web site www.tscm.com/outsideplant.html shows many examples.
We use dial-up phone lines, but nobody knows the phone numbers.	A tap on outgoing lines or detailed billing records quickly reveals every phone number dialed by the master. "War dialer" software is available on the Internet to automatically dial banks of numbers and identify those that are answered by a modem.
We use dial-back modems so that unauthorized users cannot gain access.	Once the line is tapped, dial-back is easily defeated. Other known methods do not require tapping the line.
Our systems are protected by passwords	Methods of stealing passwords are widely known. The easiest is to simply eavesdrop when the password is sent, in the clear, over the communications link. Dictionary "guessing" attacks are also common. Sharing passwords and/or never changing them is a common and dangerous practice.
We use frequency hopping spread spectrum radio, the same as the military for secure communications	There are simple methods to decode frequency-hopping sequences. The Wireless LAN Association specifically recommends using encryption on all networks, including spread spectrum. That's what the military uses - encryption.
We use a proprietary protocol so an eavesdropper couldn't understand our SCADA messages.	Even proprietary protocols are more widely known than many realize. Vendors, vendors' consultants, your current and former employees, current and former employees of other companies using the same SCADA protocol will know the details. Manuals and software tools for analyzing protocols can be downloaded from the Internet.

a. Cryptography

Despite the obvious desirability of securing control system communications, there are many challenges to accomplishing this task. Most control system field devices, such as RTUs, are designed for relatively specialized functions and do not have the computational power necessary to handle most public encryption protocols. In addition, control system messages are generally very small and are transmitted at relatively slow speeds, and often have instantaneous response

requirements; therefore the bandwidth requirements of most encryption protocols greatly exceed the bandwidth availability on most control system networks, and the latency that encryption could introduce into the message traffic could be prohibitive.

However, in spite of these obstacles, the evident necessity of secure control system communications has led the AGA to prepare a series of reports that provides recommendations for protecting those communications. AGA Report 12 provides an extensive study on the encryption of control system communications and its goal is to introduce a standard of cryptographic protection. This standard is to take the form of cryptographic modules that is immediately inserted in between a component of the control system network (such as a master station or a remote substation) and its means of transmitting and receiving data (such as a modem). Plaintext from the transmitted control system component will enter into the plaintext port of the cryptographic module and an enciphered version will be released from the ciphertext, where it will then be transmitted across the communications line. The process will be repeated, in reverse, at the receiving end. Since control system messages are simple and often repetitive, confidentiality is not a prime consideration, whereas integrity is absolutely vital. An encryption protocol for control system "must prevent an adversary from constructing unauthentic messages, modifying messages that are in transit, reordering messages, replaying old messages, or destroying messages without detection." [94] An obvious method of accomplishing this, the introduction of a message authentication code at the end of the message, would require the entire received message to be buffered by the cryptographic module so that its authenticity could be checked prior to passing the message through its plaintext port, and would introduce significant undesired latency into the system. Therefore, Cisco Systems and the Gas Technology Institute have collaborated on the authorship of a protocol that could address these problems.

The mechanism works as follows. Receipt of a plaintext message causes a transmitting cryptographic module to immediately begin sending an encrypted message header that includes a sequence number identifying the message. The message is then

sent in short blocks that are buffered and encrypted, with the final transmission being the message authentication code. Rather than buffer the entire message before checking for authentication, the receiving cryptographic module first checks a sequence number to ensure that it is correctly incremented from the last sequence received. This is the first part of the integrity check. If this sequence number is incorrect, the rest of the message is ignored. If the sequence number is correct, the cryptographic module buffers a cyber block, decrypts it, and then transmits it as plaintext at the same time it is still receiving the rest of the encrypted message. This protocol introduces minimum latency, since it adds a total of 32 characters if 128-bit encryption is used, regardless of message length. The slow speed of the communications channel means that an adversary can make only a limited amount of trials before his attempt is detected.

This protocol involves utilizing a cascade cyber that is composed of two block ciphers. Encrypting the plaintext is done using a counter mode (CTR) that depends on the message sequence number and the position of this particular block within the message, and this result is re-encrypted using electronic codebook mode (ECB). This is designed to provide strong message integrity since "forging and alteration are prevented by ensuring that an unauthentic ciphertext has a low probability of decrypting to a control system message containing a valid CRC. Reordering and replay are prevented by ensuring that an alteration of the sequence number will likewise result in a low probability that the ciphertext decrypts to a control system message containing a valid CRC." [94] This technique does not protect the system from DoS attacks—and it makes the assumption that master station as a trusted entity—but it appears to be a promising possibility of protecting the integrity of control system messages.

b. Secure Virtual Private Networks (VPN)

A secure VPN is a means of protecting information that is transmitted over a public network that utilizes insecure protocols. In theoretical terms, the VPN creates a cryptographic "tunnel" through which the data travels, and this tunnel protects the data from the insecure medium through which the data actually passes. VPNs are often secured using IPSec (for protecting OSI level 3) or SSL (for protecting OSI levels above

level 3). Since the majority of control system communications are beginning to utilize TCP/IP protocols, either IPSec or SSL could be utilized to provide protection for the communications. However, both of these protocols present some problems. SSL and IPSec utilize both utilize public keys to establish a session key, and public key encryption may introduce unacceptable latency in a SCADA system. Additionally, if one considers that the primary purpose of securing control system communications is to ensure integrity of the message traffic, both SSL and IPSec are probably far more robust than necessary, since confidentiality is one of the major focuses of both these protocols. However, it is not inconceivable that paired-down versions of these could provide adequate security to control system communications, especially if the problem of latency is not a serious one, and implementation of VPNs that utilize these protocols is far superior to continuing to send messages in the clear, with no protection whatsoever.

4. Reduce the Vulnerability of Wireless Links

The use of wireless communications in SCADA systems is increasing, and this poses significant security problems. Wireless communications are extremely vulnerable to collection by hostile individuals, and the very nature of the 802.11 protocol makes it a relatively simple matter for an attacker to launch a DoS attack simply by flooding an access point with message requests. Encryption for wireless access points, known as Wireless Encryption Protocol (WEP), has been demonstrated to have known vulnerabilities, particularly in its earlier incarnations. The latest IEE standard for wireless security, 802.11i, addresses the weaknesses of WEP but may not be suitable for control system due to its complexity, lack of accommodation for older deployed equipment, and interoperability concerns [96]. Companies that insist upon utilizing wireless communications on their control system networks should combine some version of WEP with another form of protection, such as a VPN, to ensure the security of their system.

D. IMPROVING SECURITY ADMINISTRATION

Most control systems have horrible security administration practices. Those systems that do implement some form of security administration often do not utilize effective administration that is specific for SCADA systems. Without a strong security

administration system, systematic security is impossible to achieve, because the security effort is disorganized, undirected, and is not fostered in a security-aware environment. Implementation of a strong security administration program, as outlined in brief in the following sections, will lay the foundation of a conscious, determined security effort designed to successfully reduce the system's vulnerabilities and protect the system against malicious activity.

1. Control System Security Policy

The cornerstone of any effective security administration effort is the establishment of a strong security policy. The security policy provides a clear, management-level picture of the organization's security vision, and provides the direction needed to focus the security effort. Overarching business objectives are the pillars upon which a security policy rests. Lack of a coherent security policy leads to a chaotic, ungoverned system that will inevitably have vulnerabilities and makes it impossible to sustain self-perpetuating security. Creation of a strong policy will then be used to define the particular practices to be used within the control system environment [97].

Control systems perform specialized functions and are governed by restrictions and idiosyncrasies that are far different from a standard IT network. For example, data sensitivity of a control system could be far different from that of an ordinary network. Control systems usually perform with a high-degree of time criticality of its performance. Yet another difference is that control systems may not be able to tolerate significant downtime, precluding the application of security patches. Accordingly, the policy for a control system should be specifically designed for that system and should be a completely separate document that a general security policy.

Sandia National Laboratories has developed a trademarked security policy framework that is designed to assist control system users in developing their own specific policy. The policy should describe the purpose and scope of the policy, the control system organization, the control system information architecture, categorization and ownership of control system data, and security risk management. The framework describes nine security targets and provides specific elements of the targets that the

policy authors will then detail as appropriate for their own particular system and environment. A graphical depiction of the control system policy framework is shown below in Figure 18.

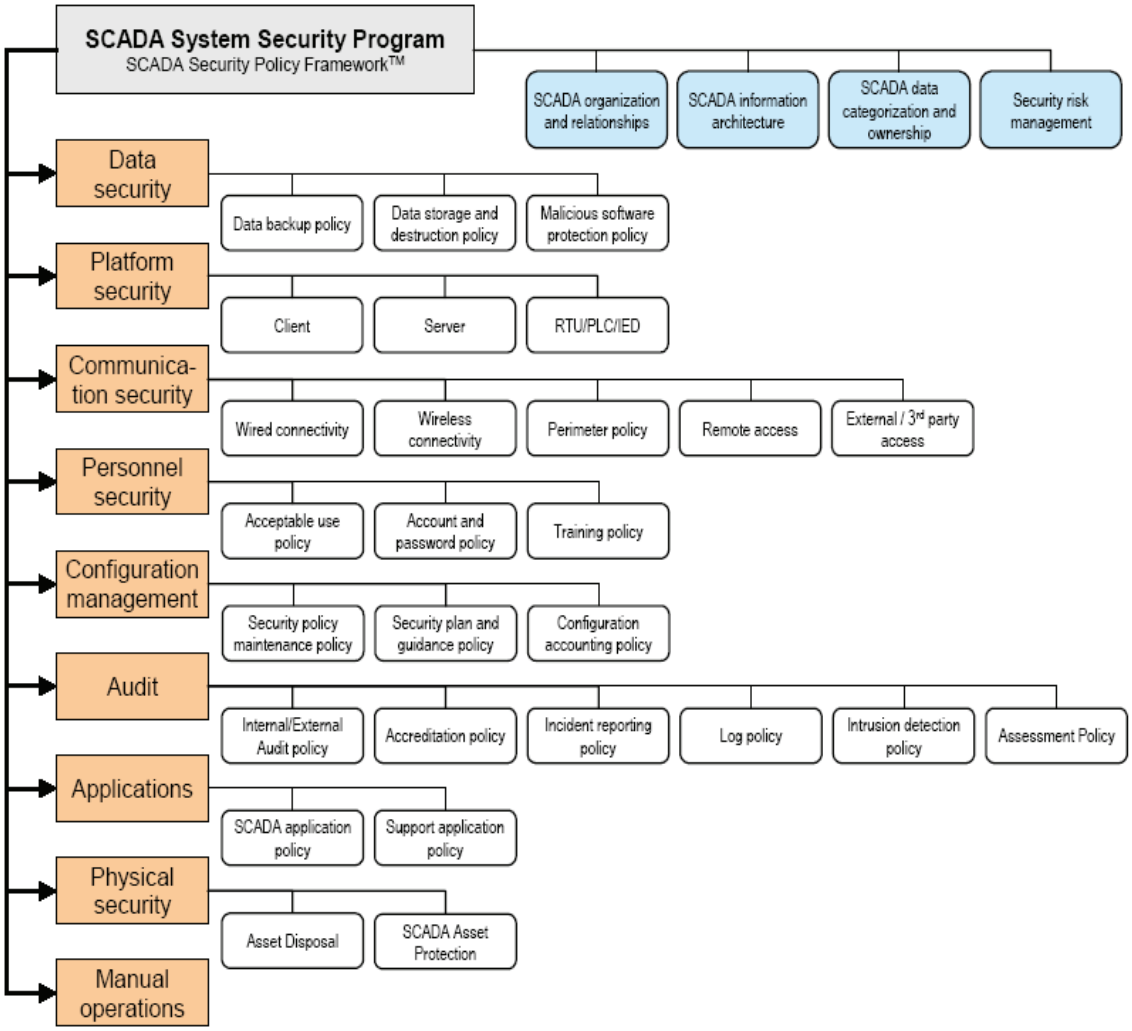

Figure 18. Control System policy framework (From [97]).

It is vitally important to write effective policies that articulate proper user practices, and to promulgate these policies to the personnel who utilize the system. Poor user behavior has become such a security concern that it is included in the 2007 SANS Top Twenty, which lists the current top twenty computer vulnerabilities as determined by the SANS Institute. Examples of this type of behavior include the connection of

unauthorized or infected devices to a network, downloading unauthorized software, and granting excessive user rights on a network. It may also include the inter-mingling of functional roles, such as giving control system administrative personnel the capability of checking email and browsing the Internet via the control system network. Clearly defining proper user activities, and ensuring that personnel understand what behavior is proscribed, is a necessary requirement to improving the security of any control system.

2. Procedures, Plans, and Training

The security policy is only the broad-brush base upon which a security program rests. A policy is a high-level document that provides guidance and direction. Implementation of that policy requires a greater level of specificity. This detail is provided by procedures and plans. Procedures and plans are based on the directives of the security policy and "must be predicated upon elements of the policy to be coherent and effective." [44] Simply put, policy explains what must be done, while procedures and plans explain how it is to be done.

Of course, all the documentation in the world is useless unless the right personnel are familiar with their contents, and, more importantly, know how to utilize them. This is where training comes in. Regular security training offers two main benefits: it provides structured instruction in the appropriate application of plans and procedures, and it creates a security-conscious atmosphere that enforces good security practices by reducing complacency.

3. Security Auditing

Good security administration is not something that can be applied on a one-time basis. A control system network, just like any other IT network, is a constantly evolving organism, and the policy and procedures that govern that organism has to be similarly fluid. A security policy must be constantly audited and reviewed in order to ensure that it accurately reflects the actual security requirements of the control system, and plans and procedures must be periodically examined to ensure that they accurately embody the principles of the policy.

4. System and Network Security Administration

Security administration does not end with the drafting of policies and procedures. An important part of security administration is the administration of the system itself, and most control systems are simply substandard in this regard. Poor system administration can lead to exploitable vulnerabilities that can allow malicious attackers free access into the network, and it is very important that these vulnerabilities are eliminated.

There are a variety of steps that a control system administrator can take to improve the security of the system. Perhaps the easiest of these is the issuance of individual user accounts to only those personnel whose responsibilities require them to have access into the system, with strong passwords that need to be changed periodically. Many control systems utilize shared accounts that are used by a variety of personnel, and are often protected with weak passwords that are in place indefinitely. This practice makes the control system vulnerable to password cracking, and promotes an atmosphere where it is "all right" to share account passwords, making it more likely that unauthorized insiders can gain access to the system. Indefinitely-maintained passwords also mean that personnel who no longer require access—such as recently-terminated personnel who may bear a grudge—are still able to access the system. Individual accounts, issued on a need-to-know basis, that require password aging and which are removed as necessary, is a good way to prevent such unauthorized access. Password data, as is the case with most other control information, is often transmitted in the clear. This makes them easy prey for snoopers who have tapped the communications line. Therefore, system administrators need to take pains to ensure that passwords are offered some form of protection prior to transmission, either by encryption or a VPN. In addition, system administrators also need to make sure that user accounts are created in such a way that the owners of those accounts do not have access to data that is beyond the sensitivity level required for the execution of their duties. System administrators also need to regularly examine network logs in order to have a running picture of what type of activity is occurring on their network, so that potential (or even successful) penetrations can be detected and responded to.

E. IMPROVING THE SECURITY OF CONTROL SYSTEM PLATFORMS

Since the control system industry is seeing such a growing transition to open computing platforms, special care must be taken to make these platforms as secure as possible. Common operating systems such as Windows and Linux have many well-publicized vulnerabilities that are easily targeted by malicious personnel. Security personnel must take the necessary steps to seal those vulnerabilities and make their machines as resistant to exploitation as possible.

Many operating systems, and other software applications, are installed on machines with default settings applied. These default settings can make the computer very vulnerable. Software that is installed on control systems should have all unnecessary services deactivated and all unnecessary ports closed. When practical, security patches should be applied to the systems in order to automatically resolve known vulnerabilities, but this should be done in an extremely cautious manner, since installation of these patches can open new security holes and can induce unpredictable and unacceptable deviation of behavior in the control system. System administrators need to ensure that all machines require password access, and that this access is conducted on an individual basis, at a privilege level that is appropriate for each particular user. Power-on and screensaver passwords need to be enabled for all machines, and strong authentication, utilizing some sort of token or biometric device in addition to a password, is highly encouraged. Critical hosts, including remote devices, need to be offered physical protection and housed in a relatively secure environment, and remote access into each machine needs to be restricted as closely as possible.

F. RECOMMENDATIONS FOR SHIPBOARD CONTROL SYSTEMS

Because of the many challenges previously discussed, it is impossible to fabricate a secure SCADA architecture that can be applied across all platforms. There is simply too much variation between ships, and too large a paucity of coordinated information about the systems on those ships, to accomplish this task. Architectures would have to be designed on a ship-by-ship basis, after careful study of the particular configuration of the

particular vessel and close cooperation with the entities that control the installation of HM&E equipment on that vessel. Such an undertaking is beyond the capability of this thesis.

The lessons learned from control systems will be extrapolated and applied to the security of ship-based, U.S. Navy control systems. What follows is a list of security recommendations based on information gleaned from the research that has been conducted for this thesis. These recommendations may be lacking in specificity but they are general enough that they should be able to be by across all Navy ships, and the security of those ship's control systems should be improved as a result.

1. Implement Certification and Accreditation

A well-organized, uniform, and concrete C&A effort is crucial for the utilization of secure control systems in the Navy. Both the DITSCAP and DIACAP were developed to provide assurance that the system being evaluated possessed a measurable level of protection and could operate in a specific environment with an acceptable level of risk. Without this assurance, there is no way to determine or define the relative security of a system. Failure to develop and, more importantly, implement an effective C&A process invalidates the intent of the DITSCAP and impairs the quantifiable expression of control system security.

A strong C&A effort is especially important when many different systems are integrated into the overall control system environment, as is the case on board a ship, where the lack of a thorough mapping of the various system interconnections can introduce security flaws that may put the system at risk. The DoD needs to shore up its C&A program by developing a program that contains system definitions, implementation requirements, and accreditation standards that can be applied across all DoD components, and the Navy needs to ensure that this program is applied to all of its shipboard control systems. Otherwise, the security of control systems will be problematic at best.

2. Incorporate Effective Access Controls

An organization cannot hope to maintain an appreciable level of information system security unless it is able to protect those systems, and the data contained within and traveling through those systems, from unauthorized access. Proper access controls are critical to fulfilling this goal. Federal information systems have significant shortfalls in this area, and preventing these shortfalls from appearing in shipboard control systems is an important part of fabricating effective control system security.

Ship-based information system security managers should ensure that their ship's control systems are protected from all manner of unauthorized access. Physical access to both the ship in general and to the control systems themselves should be vigilantly controlled. Administrative functions should be incorporated to ensure the elimination of unnecessary accounts for personnel who have transferred or changed jobs, as well as the inclusion of a password policy that requires the creation of strong passwords and mandates periodic password changes. Information flow within the control system network should be carefully monitored and the logical boundary of the control system should be maintained at all times. The capability of remote access into the system should be continually evaluated and corrected for, and the control system should be segregated from the enterprise LAN to the greatest extent possible.

In addition to protecting control systems against hostile outsiders, it is also necessary to provide restrictions to authorized insiders as well. Personnel management procedures should be instituted to ensure that the proper screening of control system personnel is rigorously executed and regularly enforced. It is also important to have clear division of duties, permissions, and responsibilities within the members of a ship's information security workforce in order to guard against usurpation of privilege. The authority to perform critical functions on a system, or to manipulate critical data, should be stringently restricted, and personnel should be given the appropriate permission level commensurate with their duties. Users should be compelled to observe the principle of least privilege at all times, and should be educated in the need to execute tasks at the lowest possible privilege level that can accomplish the tasks.

3. Development of Comprehensive Security Policies and Procedures

A well-planned and thoughtfully organized security policy provides the foundation for the security of control systems. This is the starting point for all other actions. Proper expression of the high-level standards that are expected of control system security is crucial for the development of lower level procedures that will actually illustrate the fulfillment of security requirements. Conversely, a poorly worded or incomplete security policy inevitably leads to flawed procedures and porous security.

All shipboard control systems should be governed by a security policy that is specifically written for the peculiarities of the HM&E system. Effective security measures for control systems embrace different types of security ranging from computer-based to administration. Therefore, an effective security policy that outlines HM&E security regulations should be similarly wide reaching. For example, the policy should recognize the presence of classified information within the HM&E network, how such data is controlled and labeled, and how the flow of such information must be regulated when moving between networks of dissimilar classification levels. Strict configuration management of the HM&E network, with limits on who may alter the environment or incorporate new software, should also be described in the policy. Other facets of the policy should include personnel security procedures, provisions for cleared civilian contractors and uncleared personnel, administrative security procedures such as account creation and deletion, and a description of the ship's physical security.

The Department of Defense Information Assurance Directive (DoD Directive 8500.1) lists policy requirements that are designed to promote the confidentiality, availability, and integrity of the information contained within information systems. Codification of these requirements, as well as the development of effective implementation schemes that promote and actualize the requirements, will foster an environment of control system security and will not only allow for the expression of executive-level security expectations, but will empower personnel by providing a specific set of instructions to follow which will enhance control system security.

Since security policies for information systems in general do not suffice for control systems, the previously-mentioned security policy framework from Sandia National Laboratories could be used in conjunction with DoD Directive 8500.1 to form a security policy framework that is tailored for control systems and which embraces the concepts promulgated by the DoD Information Assurance program. Guidance on drafting a security policy using this methodology is shown in Appendix A.

4. Securing Control System Platforms

The implementation of commercial off-the-shelf platforms with shipboard control systems creates many security problems. Personal computers running variants of the Windows Operating System seem to be the workstation of choice for many shipboard control system components, such as ICAS. These workstations have the advantage of being familiar to the technician, and they offer an intuitive human-to-machine interface that allows a novice user to quickly become familiar with the control system software application. However, these benefits are counterbalanced by the inherently insecure nature of the platforms.

Both Windows 2000 and Windows NT have significant security issues. Both platforms have many security vulnerabilities that, if exploited, could result in a variety of effects, including escalation of privilege, denial of service, alteration or compromise of protected data, and the execution of malicious code. The method of exploitation may be either remote or physical access, depending on the vulnerability, and a user does not always need to be an authorized user to affect an attack. These vulnerabilities are exacerbated by the default security settings of these operating systems, which are incapable of providing any appreciable measure of security. Some of these defaults include no required password length or complexity, no encrypted storage of passwords, lack of any enforced password history, undefined account lockout policy, and disabled auditing of events. These default settings are often completely incompatible with accepted security administration practices and, if left unchanged, create numerous avenues that enable successful exploitation of the known operating system vulnerabilities of the workstation. A tiny sample of these vulnerabilities is listed below in Table 9.

Since Windows is widely used in HM&E networks, the security of these platforms needs to be maximized as much as possible. Workstations need to be outfitted with security tools such as firewalls and anti-virus software, and they need to have the most recent security patches installed. Services that will not be used should be deactivated on each workstation to prevent it from being utilized by an attacker as part of an exploit. Basic security administration principles, such as strong password enforcement and mandatory password aging, should be implemented on each machine. Appendix B provides a more complete security checklist for which should be effective for both Windows 2000 and Windows NT, and which will contribute to the security of shipboard control systems and their networks.

Table 9. Some Windows 2000 and Windows NT Vulnerabilities (After [93, 94]).

WINDOWS 2000	
Vulnerability	**Assessment**
Desktop Separation Vulnerability	Could allow a malicious user to gain additional privileges on a machine that they could log onto at the keyboard.
Local Security Policy Corruption Vulnerability	Could allow a malicious user to disrupt normal operation of an affected machine, and potentially of an entire network. If a workstation or member server were attacked via this vulnerability, it would effectively remove the machine from the domain; if a domain controller were attacked, it could no longer process domain logon requests.
Malformed RPC Packet Vulnerability	If a malicious user transmits a malformed Remote Procedure Call (RPC) client packet to a Windows 2000-based computer, the RPC Server service on the host computer may stop responding
Network DDE Agent Request Vulnerability	Could, under certain conditions, allow an attacker to gain complete control over an affected machine.
WINDOWS NT	
Vulnerability	**Assessment**
Windows NT Privilege Elevation Attack	A program called SecHole (Sechole.exe) is available on the Internet that exploits a privilege elevation vulnerability in the Windows NT operating system. The program performs a sophisticated set of steps to allow a non-administrative user who is logged on locally (at the console of a system) to gain debug-level access on a system process.
Named Pipes Over RPC Issue	A vulnerability exists in the way Windows NT 4.0 handles named pipes over the Remote Procedure Call (RPC) services. An attacker could create a denial of service situation on a Windows NT 4.0 system by opening multiple named pipe connections to RPC services and sending random data.
Authentication Processing Error in Windows NT 4.0 SP4	A logic error exists in Service Pack 4 for Windows NT 4.0 that could, under certain conditions, allow a user to log on interactively and connect to network shares using a blank password.
Windows NT Screen Saver Vulnerability	Could allow a user to gain administrative privileges on a computer by running a malicious screen saver program.
Remote Registry Access Authentication Vulnerability	If a request to access the registry is malformed in a specific fashion, it could be misinterpreted by the remote registry server, causing it to fail. Because the Remote Registry server is contained within the winlogon.exe system process on Windows NT 4.0, a failure in that process would cause the entire system to fail.

5. Standardizing HM&E Equipment

The lack of a coherent Navy control system structure is a considerable roadblock to securing these systems. The effort needed to simply find information about control systems was daunting, and much of the information seemed to be either contradictory or out-of-date, requiring further investigation. The immense quantity of HM&E components within the Navy inventory illustrates an HM&E system that gives the appearance of being disorganized and cluttered. Careful consideration should be given to tidying the system up.

The Navy's HM&E system should be standardized as much as possible. It is apparent that equipment and machinery variations among ship classes add a considerable factor of complexity to any attempt of standardization. However, there are still many steps that can be taken to simplify the picture. For example, vesting management of all types of HM&E, for all classes of vessels, with a central management facility would encourage the elimination of duplicative or unnecessary systems, and would stimulate development of systems that incorporated the best of multiple systems. A standardized HMI architecture, expanded to as large a target set as possible, would reduce confusion among security administrators and provide more coherent guidance on securing the control system network. Reduction of HM&E components would further lower the complexity of the problem by limiting the number of variables that could be added to the security picture.

Despite the reluctance of the critical infrastructure industries to apply massive corrective measures to the insecurities of their systems, the strategy outlined in this section illustrates that there has been significant developmental work done on the subject. Although much work remains to be done in this area, the incorporation of the Common Criteria in control system design, the development of different control system standards, and the correction of typical network, architectural, and policy weaknesses is a good beginning for improving the security of control systems in general. The security of shipboard security control systems will be greatly enhanced by following these general recommendations, as well as implementing the more specific measures focusing on shipboard systems themselves.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. SUMMARY AND CONCLUSION

A. SUMMARY

Control systems are unquestionably essential to the well-being of the nation. They are present in the industries and activities that form the very foundations of our lives. By protecting these systems from harm, we safeguard the pillars of our society. Unfortunately, although this protection is of unparalleled importance, nobody has mustered a defensive effort commensurate with criticality of the task.

Critical infrastructure control systems possess considerable vulnerabilities and face widespread potential threats. Recent trends in computer attacks ---including the automation and sophistication of attack tools, the rapid discovery of vulnerabilities, the increasing permeability of firewalls, and the rising asymmetric threat --- and a spate of attacks against the critical infrastructure bring the severity of this problem into sharp focus. Control systems across the board typically suffer from significant network-related challenges, countless platform vulnerabilities, administration flaws, and the growing preponderance of control system information.

Shipboard control systems are remarkably similar to the control systems found within the national infrastructure. They exert considerable influence on the proper functioning of the vessel, just as national control systems exert an analogous influence on the functioning of the nation. They are also faced with similar threats, and face similar vulnerabilities, and have had similar challenges dealing with these issues. Fortunately, they can be addressed with similar solutions to these problems.

There are a number of measures that can be taken to address the control system security problem. One of these measures is the implementation of strict evaluation and certification of these systems, including the implementation of the DIACAP for shipboard control systems. The development, incorporation, and adherence of cyber standards for control systems will also go a long way towards shedding new light into

correcting the security problem. Additional measures include correcting control system network problems, improving control system security administration, and enhancing the security of control system platforms.

B. CONCLUSION

This thesis sought to demonstrate the importance of shipboard control system security, to render a judgment about shipboard control system security, and to provide some recommendations to improve that security. During this process, a sample control system security policy framework and a checklist to secure control system Windows platforms were developed. While this is a good start to addressing the control system problem, much more work needs to be done in this field. Corporations within the national critical infrastructure industry need to take the cyber threat to control systems seriously, and implement measures to combat this threat. The federal government, and the Navy in particular, needs to examine its own control systems as well and overcome the challenges that have this far led to the insecurity of these systems.

C. RECOMMENDATIONS FOR FUTURE WORK

There are other opportunities for thesis work that can be performed in this area. These include:

1. The careful examination of control system security for a single ship, including penetration testing, in order to develop a comprehensive vulnerability assessment and a detailed, vessel-specific plan for correcting any vulnerabilities that are discovered.

2. Assembling a team of personnel to examine all the ships of a particular ship class in the same manner as above. Such an approach would illustrate equipment variation, differences in security implementation, and breadth of security vulnerabilities between vessels of the same class. The results of this project, which would indicate how control system security varies among similar ships, could also prove illuminating regardless of the results.

3. The comparison of different control system architectures and software applications, in order to determine functionality overlap and assess relative security.

APPENDIX A —GUIDANCE FOR A SHIPBOARD CONTROL SYSTEM SECURITY POLICY

The security policy of a shipboard control system defines the rules governing the protection of data, services, and resources in the HM&E network. A true security policy should be tailored for the specific vessel and control system architecture found on that particular ship. Therefore, the information contained within this appendix is meant to serve only as a framework for building a shipboard control system security policy, to be molded as necessary depending upon the specific environment encountered. It is not meant to be definitive in nature.

The formulation of a shipboard control system security policy must meet two major criteria. It must be compliant with the standards of both the Department of Defense and the Department of the Navy for information assurance, and it must be designed specifically for control systems. Since there is no DoD or DoN policy governing the establishment of security policies for control systems, outside sources must be evaluated and utilized. A control system security policy framework can be combined with general DoD security requirements to create a policy that is not only compliant with all applicable policy, but which is also tailored specifically for this particular class of problem. This is the approach taken in this appendix. The security policy framework that is articulated here uses a security policy framework devised by Sandia National laboratories and incorporates it within requirements that were extrapolated from the Department of Defense Information Assurance Directive (DoD Directive 8500.1).

A. DERIVE AND CATEGORIZE DOD REQUIREMENTS

The first step in this process is to articulate the policy requirements that are to be enforced within the security policy. When devising a security policy, one must consider the elements that must be incorporated within it. Since the Navy is part of the Department of Defense, it must be governed by applicable DoD instructions. Hence, DoD Directive 8500.1 was used as the source for deriving security requirements. The

requirements articulated in this directive were closely examined, unnecessary requirements were eliminated, and those remained were modified to fit within the framework of shipboard control systems.

The DoD mandates the promotion of three major objective information assurance conditions as part of its overall information assurance effort. These conditions are achieved via the application of safeguards or the regulation of specific activities, and should be considered the pillars of the security policy for any U.S. Navy information system, and by extension, of any U.S. Navy control system. Therefore, the next step is was to categorize all the requirements within these three broad subjects, assigning each requirement a policy identification number within one of the three IA conditions.

Confidentiality is one of these IA conditions. It is a measure of assurance that information is not disclosed to unauthorized entities or processes. Table 10 illustrates some confidentiality expressions that might be found in a shipboard control system policy.

Table 10. Confidentiality Security Policy Expressions (After [99]).

Policy ID	Policy Statement	DoD Directive 8500.1 Source
CON-1	Access to shipboard control systems shall be based on need-to-know and granted in accordance with applicable laws and policies	Paragraph 4.8
CON-2	An appropriate security clearance and non-disclosure agreement are required for access to classified information	Paragraph 4.8
CON-3	The minimum requirement for access to the information system components of shipboard control systems shall be a properly administered and protected individual identifier and password	Paragraph 4.8.1
CON-4	The use of PKI certificates and biometrics for positive authentication shall be in accordance with published DoD policy and procedures.	Paragraph 4.8.2
CON-5	Authorized users who are contractors, DoD direct or indirect hire foreign national employees, or foreign representatives shall always have their affiliation displayed as part of their e-mail addresses.	Paragraph 4.10
CON-6	Access to Navy-owned, -operated or -controlled web sites containing official shipboard control system information shall be granted according to reference (o) and need-to-know rules established by the information owner	Paragraph 4.11.1
CON-7	Shipboard control systems shall regulate remote access and access to the ship's HM&E network by employing positive technical controls such as proxy services and demilitarized zones (DMZ), or through systems that are isolated from all other information systems through physical means	Paragraph 4.12

Integrity is the second objective information assurance condition. It is that aspect of an information system that reflects the logical correctness and reliability of the operating system. It also is an expression of the logical completeness of hardware and software-implemented protection mechanisms, as well as the consistency of the data structures [98]. Integrity may be more narrowly defined as protection against unauthorized modification or destruction of information, and some possible integrity-related expressions are shown in Table 11.

Table 11. Integrity Security Policy Expressions (After [99]).

Policy ID	Policy Statement	DoD Directive 8500.1 Source
IN-1	IA requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all U. S. Navy shipboard control systems	Paragraph 4.1
IN-2	All shipboard control systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities the trustworthiness of the users and interconnecting systems; the impact of impairment or destruction to the information system; and cost effectiveness	Paragraph 4.2
IN-3	Information assurance shall be a visible element of all investment portfolios, incorporating Department of Defense (DoD) -owned or -controlled shipboard control systems to include outsourced business processes supported by private sector control systems and outsourced information technologies; and shall be reviewed and managed relative to contributions to mission outcomes and strategic goals and objectives	Paragraph 4.3
IN-4	All shipboard control systems shall be certified and accredited	Paragraph 4.13
IN-5	Interconnections between shipboard control systems with information systems of different security domains shall be employed only to meet compelling operational requirements. Secure configurations of approved IA and IA-enabled IT products, uniform risk criteria, trained systems security personnel, and strict configuration control shall be employed.	Paragraph 4.14.3
IN-6	All personnel authorized access to shipboard control systems shall be adequately trained in accordance with DoD and DoN policies and requirements and certified as required in order to perform the tasks associated with their IA responsibilities	Paragraph 4.19
IN-7	Individuals shall be notified of their privacy rights and security responsibilities, in accordance with U. S. Navy General Counsel-approved processes, when attempting to access shipboard control systems	Paragraph 4.23

Availability is the third objective information assurance condition. When considered within the context of security, availability is generally defined as the capability for authorized users to have timely, reliable access to data and information

services. Every security policy must address the aspect of availability in some degree. Some possible availability-related elements of a shipboard control system security policy are listed in Table 12.

Table 12. Availability Security Policy Expressions (After [99]).

Policy ID	Availability Policy Expressions	DoD Directive 8500.1 Source
AV-1	Interoperability and integration of shipboard control system IA solutions shall be achieved through adherence to an architecture that will enable the evolution to network centric warfare. This combination produces layers of technical and non-technical solutions that: provide appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, to include robust key management and incident detection and response.	Paragraph 4.4
AV-2	The ship shall organize, plan, assess, train for, and conduct the defense of shipboard computer networks (including control systems) as integrated computer network defense (CND) operations that are coordinated across multiple disciplines	Paragraph 4.5
AV-3	Information assurance readiness shall be monitored, reported and evaluated as a distinguishable element of mission readiness	Paragraph 4.6
AV-4	The information system components of all U.S. Navy control systems shall be assigned a mission assurance category that is directly associated with the importance of the information they contain relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Requirements for availability and integrity are associated with the mission assurance category, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know	Paragraph 4.7
AV-5	All interconnections of shipboard control systems shall be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems	Paragraph 4.14
AV-6	All shipboard control systems shall comply with DoD ports and protocols guidance and management processes, as established	Paragraph 4.15
AV-7	All IA or IA-enabled IT hardware, firmware, and software components or products incorporated into shipboard control systems must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase	Paragraph 4.17
AV-8	All IA and IA-enabled IT products incorporated into shipboard control systems shall be configured in accordance with security configuration guidelines approved by the Department of Defense and the Department of the Navy (DoN)	Paragraph 4.18
AV-9	Public domain software products and other software products with limited or no warranty, such as those known as shareware of freeware, shall only be used in shipboard control systems to meet compelling operational requirements. Such products shall be thoroughly assessed for risk and accepted for use by the responsible DAA	Paragraph 4.19
AV-10	Identified shipboard control system vulnerabilities shall be evaluated for DoD impact and tracked and mitigated in accordance with DoD-directed mitigation	Paragraph 4.21

B. MAP REQUIREMENTS TO SECURITY POLICY FRAMEWORK

Determining the security requirements was not sufficient to construct a security policy. The requirements from DoD Directive 8500.1 were applicable to all DoD information systems, not just control systems. Deriving requirements from that directive was a good starting point, but now these requirements had to be applied in a document that was tailored for the unique considerations of a control system security policy. This was where the Sandia model came into play.

Depicted graphically previously in Figure 18, the Sandia Laboratories control system security policy is designed to provide a control-system specific security policy that will "ensure that all the specialized features, needs, and implementation idiosyncrasies of the… system are adequately covered." [98] It describes the control system's operation, its relationship to other systems and operations, the boundaries of the system, data categorization, and risk management. It also lists nine major security sections that address various portions of the security policy. These sections are data security, platform security, communications security, personnel security, configuration management, auditing, applications, physical security, and manual operations. The plan is designed to be scalable and adaptable to the requirements of the organization. It is by no means an authoritative diagram of control system security, but should be general enough to provide system administration personnel a general idea of how to proceed.

This step in developing the security policy entailed taking the requirements that were derived from DoD Directive 8500.1, and labeled according to their satisfaction of confidentiality, integrity, and availability, and incorporating them within the Sandia framework. This was accomplished by mapping the requirements to the nine different security sections and their subsections. It is important to note that the requirements are actually a subset of the content of a security policy, so not all the pieces of the policy will be able to be mapped to the requirements. Virtually all of the requirements, however, should be able to be mapped to the policy. The following sections go into this in more detail by examining the sections of the security policy as taken directly from the Sandia framework.

1. Data Security Policy

The data security policy determines the treatment of defined data categories. Different data categories may have distinct requirements for protection, which should be specified in this policy. All forms of data (be they paper, digital, video, etc.) must be protected commensurate with their criticality to the system. Data marking and need-to-know controls are important considerations [97].

Table 13. Data Security Policy Expressions (After [97]).

Category	Policy Expressions	DoD Directive 8500.1 Policy Expressions Satisfied (if Applicable)
Data Backups	This policy will define all of the details concerning what data must be backed up, how often, and where the backups will be stored. The retention schedule for the backups will also be identified. If there are classes of devices which will be exempt from backup requirements, they must be identified.	N/A
Data Storage and Destruction	Data must be protected during its complete lifecycle, including creation, storage, and destruction. Destruction is as important as creation and storage, and it is often an adversary's easiest means of data theft.	AV-4
Malicious Software Protection	Malicious code can cause irreparable harm to any computer system by either stealing or destroying data. Controls must be set forth which prevent the inadvertent or intentional installation of any malicious code.	AV-7, AV-8, AV-9, AV-10

2. Platform Security Policy

Platform security will identify required secure configuration defaults and will specify account creation and termination procedures. Separate definitions for a secure configuration will be detailed for clients, servers, and end devices (RTU/PLC/IED). Important concepts such as virus checking, intrusion detection, access control, and encryption must be addressed [97].

Table 14. Platform Security Policy Expressions (After [97]).

Category	Policy Expressions	DoD Directive 8500.1 Policy Expressions Satisfied (if Applicable)
Client	Rules governing secure client specification	CON-1, CON-2, CON-3, CON-4 CON-6, AV-3, AV-6, AV-7, AV-8, AV-9, AV-10
Server	Rules governing secure server specification	CON-1, CON-2, CON-3, CON-4 CON-6, AV-3, AV-6, AV-7, AV-8, AV-9, AV-10
RTU/PLC/IED	Rules governing secure RTU/PLC/IED specification	CON-1, CON-2, CON-3, CON-4 CON-6, AV-3

3. Communications Security Policy

Communication security identifies the paths that data will take through a network, details protection mechanisms for different network segments, identifies security zones, and specifies external connection permissions [97].

Table 15. Communications Security Policy Expressions (After [97]).

Category	Policy Expressions	DoD Directive 8500.1 Policy Expressions Satisfied (if Applicable)
Wired	This section defines how to communicate within the wired portions of the automation network, including all parts of its LAN or WAN segments. Cryptographic requirements are specified based on data categorizations.	AV-5, AV-6, IN-5
Wireless	Wireless connections to a network will need to have special consideration due to the broadcast nature of the medium. This section should designate what type(s) of data may traverse the wireless network, and how connections to the network will be established. Also, the acceptable configurations for wireless connections to the wired network are specified. Schedules and responsibilities for wireless coverage assessments will be here.	AV-5, AV-6, IN-5
Perimeter	This policy specifies how data is input and output from the control system with other networks. The types of controls needed and the location of these controls will be identified. Security zones will be specified which will help to determine the cryptographic controls needed.	AV-5, AV-6, IN-5
Remote Access	Here is defined if and how users can connect to the automation system from remote locations. Remote access is often a requirement in geographically large installations to effectively maintain the system. Vendors also use remote access for off-site maintenance and product upgrades. This policy details how to request access, who approves the access, and any time restrictions for the access.	AV-5, AV-6, CON-4, CON-7
External/3rd Party Connections	This section specifies if, when, and how outsiders will access information and equipment on the automation network. This policy details how to request access, who approves the access, and any time restrictions for the access. The monitoring and logging requirements will be stipulated, as well as prohibited actions. If there are time, equipment, or other requirements, these will also be enumerated.	AV-5, AV-6, CON-5

4. Personnel Security Policy

Workers on the automation network will have different functions and security needs compared to others on the conventional IT network. This policy will express the job requirements and hiring policy for control system staff. It will also differentiate the different functions and security requirements for control system personnel, as compared to personnel who maintain the conventional enterprise LAN. These requirements may include citizenship and educational requirements, qualifications, background investigations, and clearance needs [97].

Table 16. Personnel Security Policy Expressions (After [97]).

Category	Policy Expressions	DoD Directive 8500.1 Policy Expressions Satisfied (if Applicable)
Acceptable Use	This policy defines what users can and cannot do with equipment and network resources. Due to the criticality of the control system, personal use should not be allowed on this equipment. Software on the control system network should be control-system-specific. Any access to other networks, network monitoring, and a statement detailing what the SCADA system entails must be stated here. A 'rules of behavior' document should be created which every employ is required to read and sign.	CON-1, CON-3, IN-7
Accounts and Passwords	The account and password policy will describe proper care of passwords and accounts including storage, creation, and sharing. Some policies will give minimum requirements concerning the format for passwords, while other will simply state that the current best practice must be used. Any shared passwords (for example admin passwords on equipment) will have special protections regarding creation, storage, and change requirements.	CON-1, CON-2, CON-3, CON-6
	Account creation and destruction policies will explain how users may use their accounts, and who is responsible for creating and removing accounts. Account creation must be individual for accountability purposes and based on job function. Any additional protection requirements such as screen.	CON-1, CON-2, CON-6
Training	Staff must be familiar with the security needs of the system and understand why the security controls are in place. When staff understands why they do something, they are less likely to circumvent the protections. This policy will list what training is required, the frequency of training, and who must be trained. If specialized training is required for certain staff positions, those requirements must be listed here. Contractors should receive training commensurate with permanent staff training.	IN-6

5. Configuration Management

The configuration management policy ensures the implementation of a sustainable configuration management process. The policy will list the necessary documentation and processes needed to achieve a sustainable security system. This documentation will express details regarding the revision process, timelines for security plans, policies, implementation guidance, and elements of change control and change evaluation [97].

Table 17. Configuration Management Policy Expressions (After [97]).

Category	Policy Expressions	DoD Directive 8500.1 Policy Expressions Satisfied (if Applicable)
Security Policy Maintenance	Specific plans for security policy maintenance	IN-1, IN-2, IN-3
Security Plan and Guidance	Specific plans for security plan and guidance	IN-1, IN-2, IN-3
Configuration Accounting	Specific plans for configuration accounting	IN-3

6. Applications Policy

The application policy ensures the proper configuration and use of all applications. It ensures that application use is commensurate with the security needs of the automation system, and will cover the details of program-level access control, application training, and test and development requirements [97].

Table 18. Applications Policy Expressions (After [97]).

Category	Policy Expressions	DoD Directive 8500.1 Policy Expressions Satisfied (if Applicable)
Control System Applications	Control-system-specific applications will at times have requirements for administrator access. These applications may also allow data separation, separate user logins, and password protections. This section will focus only on those applications which are written to interface with control system devices and functionality.	Dependent upon the applications
Support Applications	Support applications such as office software, databases, and logging will need to have a different set of security guidelines. The applications usually do not interface directly with control system equipment and automation functions, but may reside on the same computers or networks where control system applications are running.	Dependent upon the applications

7. Audit Policy

The audit policy defines the scope of auditing and assessment activities. Audits will determine if the protections which are detailed in policy, security plans, and implementation guides are being correctly put into practice on the system. Assessments ensure that the protections on the system are adequate for the information and functionality. Personnel who are responsible for scheduling and reviewing audits must be identified, and auditing schedules are outlined [97].

Table 19. Audit Policy Expressions (After [97]).

Category	Policy Expressions	DoD Directive 8500.1 Policy Expressions Satisfied (if Applicable)
Internal/External Audit	Both internal and external audits have an important place in a comprehensive risk management program. This section will give the details of each type of audit as well as identifying the internal organization responsible for performing or contracting for the required audits.	AV-1, AV-3
Accreditation	If an organization must be accredited, this section of the policy will give the details of the responsible parties, timelines, and participating entities.	IN-4
Incident Reporting	The individuals who are responsible in the event of an incident will be identified here. If there is a chain of reporting that must be followed, those details must be captured here. The protection level of the incident details are defined so the results and reports will be protected at the appropriate level. An incident response procedure must be developed to address issues of evidence preservation, investigation authority, reporting requirements, etc.	AV-1, AV-2, AV-3
Logging	This policy will define the logging requirements such as what will be logged, storage requirements, and revision requirements.	AV-1, AV-3
Intrusion Detection	Intrusion detection is an important tool for detection of anomalous behavior. Control system operations will require specific policies regarding its requirements and limitations for IDS.	AV-8
Assessments	The assessment portion of this policy will specify the responsible parties, timelines, and data protection for assessments performed.	N/A

8. Physical Security Policy

The physical security policy documents how control system equipment is protected from physical damage, unauthorized access, or destruction. Access to any equipment by visitors and personnel must be controlled and monitored [97].

Table 20. Physical Security Policy Expressions (After [97]).

Category	Policy Expressions	DoD Directive 8500.1 Policy Expressions Satisfied
Asset Disposal	Physical asset disposal is critical. Physical equipment must be sanitized before it can be released from the control of the system. This policy will express the guidelines and requirements for users who have physical assets that are no longer necessary. Important concepts are sanitization, tracking, and disposal technology.	IN-2
Asset Protection	Statement of protection guidelines	CON-1, CON-2

9. Manual Operations Policy

Due to the critical nature of HM&E systems, control system functions must still be performed even in the event of system failure. The manual operations policy will articulate procedures to implement this activity, and will include: manual backup procedures, chain of command, periodic inspection, training in manual operations, tests and drills on manual operation procedures, and a disaster recovery policy [97].

Table 21. Manual Operations Policy Expressions (After [97]).

Category	Policy Expressions	DoD Directive 8500.1 Policy Expressions Satisfied (if Applicable)
Manual Operations	Functions that must be performed in the event of a failure of the automated capability of the system.	N/A

Once this mapping is complete, the control system administrator has an outline to follow that incorporates DoD-level IA requirements within a policy template that is designed specifically for control systems. The next, and final, step is to write the actual policy. This is done in accordance with the specific systems employed, as well as the particular HM&E environment, and must be tailored for each the particular ship.

APPENDIX B —SECURITY CHECKLIST

WINDOWS SETTINGS CONFIGURATION CHECKLIST		
BACKGROUND AND PREPARATION		
Steps	Details and/or recommendations	
Read any applicable security policies for your organization	Determines how to implement security in accordance with requirements	
Review your user education and training plans	Ensure users will receive proper security training	
Ensure users will receive proper security training	Decide what services may be enabled and which may be deactivated	
INITIAL CONFIGURATION AND SET-UP		
Steps	Details and/or recommendations	
Ensure that all disk partitions are formatted with NTFS	NFTS offers access controls and protections that aren't available with other file system	
Enable hardware boot protection	Remove floppy and/or CD-ROM drives to prevent booting from them	
	Set BIOS restrictions to boot sources, if supported	
	Physical lock on floppy drive	
Remove or unbind unnecessary protocols	Prevents denial-of-service attacks against the protocol and safeguards against protocol-specific exploits	
Remove additional operating systems	Also applicable to unneeded subsystems	
Install latest Service Pack and post-Service Pack hotfixes	Ensures machine is equipped with latest security updates	
Disable unnecessary services	Eliminate vulnerability to service-specific exploit	
ACCOUNT POLICIES		
Steps	Details and/or recommendations	
Properly Establish Administrator Account	Ensure the Administrator account has a strong password	
	Rename the account using a non-obvious name	
	Set up a decoy "Administrator" account with no privileges	
	Enable account lockout on the actual Administrator account	
	If part of a network is administered by a domain Administrator, disable the local machine's Administrator account	
Establish Password Policies	Enforce password history	Set a limit on how often passwords may be re-used.
		Recommend 24 passwords remembered
	Establish minimum password age	Minimum password age is length of time users must keep a password before they can change it.
		Recommended minimum age is 2 days

WINDOWS SETTINGS CONFIGURATION CHECKLIST		
ACCOUNT POLICIES (cont.)		
Steps	Details and/or recommendations	
Establish Password Policies (cont.)	Establish maximum password age	Length of time users can keep their passwords before they have to change it.
		Recommended maximum age is between 42 days and 90 days
	Set minimum password length	Set the minimum number characters required for user passwords
		Recommended minimum length: 8 characters
	Set minimum password complexity	Requires the use of complex (strong) passwords. This means the password has sufficient length, is alphanumeric in structure with a mixture of upper and lower case letters, and uses at least one special character
Establish Account Lockout Policies	Account Lockout Duration	Locks account for a specified period of time.
		Recommend at least 30 minutes
	Account Lockout Threshold	Set the number of bad login attempts allowed before locking the account.
		Recommend 3 attempts
	Reset Account Lockout Counter	Set how long the lockout threshold is maintained before being reset
		Recommend 30 minutes
AUDIT POLICIES		
Set Audit Policies To…	More Detailed Description	
Audit Account Logon Events	Audit account logon/logoff events from another computer in which this computer is used to validate the account.	
Audit Account Management	Audit account management activities	
Audit Directory Service Access	Audit access to an Active Directory object that has its own system access control list specified	
Audit Logon Events	Audit local or network logon/logoff events to this computer.	
Audit Object Access	Audit access to an object--for example, a file, folder, registry key, or printer, which has its own system access control list specified.	
Audit Policy Change	Audit a change to user rights assignment policies, audit policies, or trust policies.	
Audit Privilege Use	Audit each instance of a user exercising a user right	
Audit Process Tracking	Audit when a user restarts or shuts down the computer or when an event occurs that affects either the system security or the security log.	
Audit System Events	Audit detailed tracking information for events.	

WINDOWS SETTINGS CONFIGURATION CHECKLIST	
ASSIGNMENT OF USER ACCESS RIGHTS	
Description of User Right	Details and/or recommendations
Access this computer from network	Determines which users are allowed to connect over the network to the computer.
	Assign to: Authenticated users who need remote access to the workstation
Act as part of the operating system	Allow a process to authenticate as a user and thus gain access to the same resources as a user
	Assign to: No one
Add workstations to domain	Allows a user to add a computer to a specific domain.
	Assign to: Administrators
Back up files and directories	Allows the user to circumvent file and directory permissions to backup the system.
	Assign to: Trusted users
Bypass traverse checking	Allows the user to pass through folders to which the user otherwise has no access.
	Assign to: Assign to: Trusted users
Change the system time	Allows the user to set the time for the internal clock of the computer
	Assign to: No one
Create a pagefile	Allows the user to create and change the size of a pagefile.
	Assign to: Trusted users
Create a pagefile	Allows a process to create an access token.
	Assign to: No one
Create a token object	Allow a process to create a directory object in the Windows object manager.
	Assign to: No one
Create permanent shared objects	Allows the user to attach a debugger to any process
	Assign to: No one
Debug programs	Allows a user to shut down a computer from a remote location on the network.
	Assign to: Trusted users
Force shutdown from a remote system	Allows a process to generate entries in the security log.
	Assign to: No one
Generate security audits	Allows a process that has Write Property access to another process to increase the processor quota that is assigned to the other process.
	Assign to: Administrators
Increase quotas	Allows a process that has Write Property access to another process to increase the scheduling priority that is assigned to the other process.
	Assign to: Administrators
Increase scheduling priority	Allows a user to install and uninstall Plug and Play device drivers.
	Assign to: Administrators
Load and unload device drivers	Assign to: Administrators
Lock pages in memory	Allows a process to keep data in physical memory, which prevents the system from paging data to virtual memory.
	Assign to: No one

WINDOWS SETTINGS CONFIGURATION CHECKLIST	
ASSIGNMENT OF USER ACCESS RIGHTS (cont.)	
Description of User Right	Details and/or recommendations
Log on as a batch job	Allows a user to log on by using a batch-queue facility.
	Assign to: Trusted users
Log on as a service	Allows a security principal to log on as a service.
	Assign to: Trusted users
Log on locally	Allows a user to log on locally at the computer's keyboard.
	Assign to: Trusted users
Manage auditing and security log	Allows a user to specify object access auditing options for individual resources such as files, Active Directory objects, and Registry keys.
	Assign to: Administrators
Modify firmware environment values	Allows modification of system environment variables either by a process through an API or by a user through the System Properties applet.
	Assign to: Administrators
Profile single process	Allows a user to run Microsoft Windows NT and Windows 2000 performance monitoring tools to monitor the performance of non-system processes.
	Assign to: Administrators
Profile system performance	Allows a user to run Microsoft Windows NT and Windows 2000 performance monitoring tools to monitor the performance of system processes.
	Assign to: Administrators
Replace a process level token	Allows a parent process to replace the access token that is associated with a child process.
	Assign to: No one
Restore files and directories	Allows a user to circumvent file and directory permissions when restoring backed-up files and directories and to set any valid security principal as the owner of an object.
	Assign to: Administrators and Trusted Users
	Assign to: Authenticated users
	Assign to: Administrators
SECURITY OPTIONS (cont.)	
Options	Details and/or recommendations
Additional Restrictions for Anonymous Connections	Do not allow enumeration of SAM accounts and shares
Allow Server Operators to Schedule Tasks Disabled	Disable this option
Allow System to be Shut Down Without Logon Without Having to Log On	Disable this option
Allowed to Eject Removable NTFS Media	Only Administrators should be able to do this.
Amount of Idle Time Required Before Disconnecting a Session	Maintain default of 15 minutes
Audit the Access of Global System Objects	Enabled this option, but only when there is a strict audit management process in place.

WINDOWS SETTINGS CONFIGURATION CHECKLIST	
SECURITY OPTIONS (cont.)	
Options	Details and/or recommendations
Audit the Use of Backup and Restore Privilege	Enable this option, but only when there is a strict audit management process in place.
Automatically Log Off Users When Logon Time Expires	Enable this option.
Automatically Log Off Users When Logon Time Expires	Enable this option.
Clear Virtual Memory Pagefile When System Shuts Down	Enable this option.
Digitally Sign Client Communications (Always)	Disable this option.
Digitally Sign Client Communications (When Possible)	Enable this option.
Digitally Sign Server Communications (Always)	Disable this option.
Digitally Sign Server Communications (When Possible)	Enable this option.
Disable CTRL+ALT+ DEL Requirement for Logon	Enable this option.
Do Not Display Last User Name in Logon Screen	Enable this option.
LAN Manager Authentication Level	Only enable LanManager Version 2
Message Text for Users Attempting to Log On	Set a warning banner as per local policy requirements.
Message Title for Users Attempting to Log On	Set a warning banner as per local policy requirements.
Number of Previous Logons to Cache (In Case Domain Controller is not Available)	Cache should be set to 0 logons.
Prevent Users from Installing Print Drivers	Enable this option.
Prompt User to Change Password Before Expiration	Recommended 14 days
Recovery Console: Allow Automatic Administrative Logon	Disable this option.
Recovery Console: Allow Floppy Copy and Access to all Drives and all Folders	Disable this option.
Rename Administrator Account	Change and safeguard the recorded account name.
Rename Guest Account	Change and safeguard the recorded account name.
Restrict CD-ROM Access to Locally Logged-On User Only	Enable this option.
Restrict CD-ROM Access to Locally Logged-On User Only	Enable this option.
Restrict Floppy Access to Locally Logged-On User Only	Enable this option.

WINDOWS SETTINGS CONFIGURATION CHECKLIST	
SECURITY OPTIONS (cont.)	
Options	Details and/or recommendations
Secure Channel: Digitally Encrypt or Sign Secure Channel Data (Always)	Disable this option.
Secure Channel: Digitally Encrypt or Sign Secure Channel Data (When Possible)	Enable this option.
Secure Channel: Digitally Sign Secure Channel Data (When Possible)	Enable this option.
Secure Channel: Require Strong (Windows 2000 or later) Session Key	Disable this option.
Send Unencrypted Password to Connect to Third-Party SMB Servers	Disable this option.
Shut Down System Immediately if Unable to Log Security Audits	Disable this option., since ship's systems are affected
Strengthen Default Permissions for Global System Objects (e.g., Symbolic Links)	Enable this option.
Unsigned Driver Installation Behavior	Set to Warn but allow installation.
Unsigned Non-Driver Installation Behavior	Set to Warn but allow installation.
SETTINGS FOR EVENT LOGS	
Steps	Details and/or recommendations
Maximum Application Log Size	512 kilobytes.
Maximum Security Log Size	Depends on the amount of expected activity, the amount of available disk space, and the frequency with which the logs will be manually reviewed, archived, and cleared.
Maximum System Log Size	512 kilobytes.
Restrict Guest Access to Application Log , Security Log, and System Log	Enable this option.
Retain Application Log, Security Log, and System Log	Recommend at least 7 days.
Shut Down the Computer When the Security Audit Log is Full	Do not enable.
ADDITIONAL SECURITY SETTINGS	
Disable DirectDraw**.**	
Disable Unnecessary Devices.	
Protect kernel Object Attributes.	
Restrict Null Session Access.	
Restrict Null Session Access Over Named Pipes.	

WINDOWS SETTINGS CONFIGURATION CHECKLIST
ADDITIONAL SECURITY SETTINGS (cont.)
Prevent Interference of the Session Lock from Application Generated Input.
Generate an Audit Event when the Audit Log Reaches a Percent Full Threshold**.**
Harden the TCP/IP Stack Against Denial of Service Attacks**.**
Make Screensaver Password Protection Immediate.
Disable LMHash Creation.
Disable Autorun.
Generate Administrative Alert when the Audit Log is Full..
Back up the Administrator's Encryption Certificate
Enable Automatic Screen Lock Protection.
Update the System Emergency Repair Disk **.**
Make sure the Guest account is disabled.
Restrict the use of LanManager authentication.
Secure base objects.
Protect files and directories.
Protect the Registry.
Apply appropriate Registry ACLs.
Restrict access to public Local Security Authority (LSA) information.
Restrict untrusted users' ability to plant Trojan horse programs.
Disable caching of logon information.
Set the paging file to be cleared at system shutdown.
Restrict floppy drive and CD-ROM drive access to the interactive user only.
Modify user rights membership.
Change the Scheduler service's security context.
Hide the name of the last logged-in user.
Update the system Emergency Repair Disk.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] United States General Accounting Office, *Critical Infrastructure Protection: Challenges in Securing Control Systems*, GAO-04-140T, October 2003. Available at www.gao.gov/new.items/d04140t.pdf (June 2005).

[2] Michael P. Ward, *An Architectural Framework for Describing Supervisory Control and Data Acquisition (SCADA) Systems*, Master's Thesis, Naval Postgraduate School, Monterey, CA, September 2004.

[3] Dennis J. Gaushell, and Henry T. Darlington, "Supervisory Control and Data Acquisition," *Proceedings of the IEE*, Volume 75, Issue 12, December 1987.

[4] Dennis J. Gaushell, and Wayne R. Block, "SCADA Communication Techniques and Standards," *Computer Applications in Power*, IEEE, Volume 6, Issue 3, July 1993.

[5] Synchrony White Paper, *Trends in SCADA for Automated Water Systems*, November 2001. Available at http://www.synchrony.com/trends_SCADA.pdf (June 2005).

[6] Process Automation Website: http://www.processauto.com/SCADAExamples.htm (July 2005).

[7] Jacques Beneat, Companion slides for *Vulnerabilities in SCADA Systems*, Norwich University, slide 20. Available at http://www2.norwich.edu /jbeneat/scada/scada_2003/documents/315,20,MTU Software Functions (June 2005).

[8] Robert H. McClanahan, "The Benefits of Networked SCADA systems utilizing IP-enabled Networks," *IEEE Industry and Applications Magazine*, March/April 2003. Available at http://ieeexplore.ieee.org/iel5/2943/26528/01180947.pdf?tp=&arnumber=1180947 &isnumber=26528 (July 2005).

[9] Perry Sink, "A Comprehensive Guide to Industrial Networks, Part 1: Why Use an Embedded Network or Fieldbus, and What Are the Most Popular Standards?" *Sensors Magazine*, Volume 18, Issue 8, August 2001. Available at http://www.sensorsmag.com/articles/0601/28/main.shtml (July 2005).

[10] Symantec White Paper, *Understanding SCADA System Vulnerabilities*. Available at https://enterprisesecurity.symantec.com/Content/displaypdf.cfm?SSL=YES&PDFID=652 (June 2005).

[11] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, December 2001. Available at http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf (July 2005).

[12] Steven M. Rinaldi, Companion slides for *Critical Infrastructure Interdependencies*, Sandia National Laboratories, slides 4 and 9.

[13] Alan Gunnerson, *Information Technology (IT) Security for Supervisory Control and Data Acquisition (SCADA) Systems*, University of Dallas Graduate School of Management, 15 June 2003. Available at http://cipp.gmu.edu/archive/127_DallasGunnerson_SCADA.pdf (July 2005).

[14] William J. Clinton, *Critical Infrastructure Protection*, Presidential Decision Directive 63, 18 May 1998. Available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (May 2005).

[15] George W. Bush, *Executive Order Establishing the Office of Homeland Security and the Homeland Security Council*, Presidential Executive Order 13228, 08 October 2001. Available at http://www.fas.org/irp/offdocs/eo/eo-13228.htm (July 2005).

[16] United States Patriot Act of 2001, 24 October 2001. Available at http://www.epic.org/privacy/terrorism/hr3162.html (01 August 2005).

[17] United States Office of Homeland Security, *National Strategy for Homeland Security (Executive Summary)*, July 2002. Available at http://www.whitehouse.gov/homeland/book/sect1.pdf (July 2005).

[18] United States Department of Homeland Security, *National Strategy for Securing Cyberspace*, February 2003. Available at http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf (August 2005).

[19] ISAC Council White Paper, *The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection*, January 2009. Available at http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf (June 2009).

[20] Website: "About the MS-ISAC," 10 June 2009. Available at http://www.msisac.org/about/. (June 2009)

[21] Press Release, Office of the Assistant Secretary of Defense (Public Affairs), 26 April 1996. Available at http://www.defenselink.mil/contracts/1996/c042696_ct242-96.html (July 2005).

[22] United States Air Force, "Edwards Air Force Base Digital Airport Surveillance RADAR Environmental Assessment," June 2002. Available at http://ast.faa.gov/lrra/environmental/Edwards_AFB_Digital_Airport_Surveillance_Radar_EA.pdf (July 2005).

[23] Website: "AQUIS Project at Fort Drum Recognized as an ERDC Weekly Accomplishment," 08 December 2003. Available at http://www.7t.dk/aquis/default.asp?lan=GB&shownewsid=253&title=AQUISProjectatFortDrumRecognizedasanERDCWeeklyAccomplishment (July 2005).

[24] Website: "Installation of a Wastewater Monitoring SCADA System at Fort Bragg, NC," June 2004. Available at http://www.stormingmedia.us/58/5829/A582924.html (July 2005).

[25] Website: "SCADAware Provides Control and SCADA Systems to Military for Deployable Power Plants," October 2004. Available at http://www.automation.com/store/pdetails12460.php?x=1&pagePath=00000000,00000307,00001196,00001686 (July 2005).

[26] Pacific Northwest National Laboratory, PNNL –SA- 36040, *USMC Bases Apply Latest Technology to Manage Energy Resources*, by Richard Meador, March 2002. Available at http://www.pnl.gov/dsom/publications/36040.pdf (July 2005).

[27] Barbara Quinn, "P2/Sustainability: From Preventive to Condition-based Maintenance," *Pollution Engineering*, 01 August 2001. Available at http://www.pollutioneng.com/CDA/ArticleInformation/features/BNP__Features__Item/0,6649,107435,00.html (August 2005)

[28] EDG Website: http://www.edg.co.uk/control-facilities.htm (31 July 2005).

[29] David Marques, Neil Hiller, and John Galvagno, "U.S. Navy steams into 21st Century," *InTech*, December 1997. Available at http://findarticles.com/p/articles/mi_qa3739/is_199712/ai_n8760657/?tag=content;col1 (July 2009).

[30] Dan Bensilisha, "A Tight Ship", *Fortnightly's Energy Customer Management*, Fall 2001. Available at http://www.itron.com/publications/1302.pdf (June 2003).

[31] Vernon Clark, "Sea Power 21: Projecting Decisive Joint Capabilities," *Proceedings*, October 2002. Available at http://www.navy.mil/palib/cno/proceedings.html (September 2005).

[32] United States General Accounting Office, GAO-03-520, *Military Personnel: Navy Actions Needed to Optimize Crew Size and Reduce Total Ownership Costs*, June 2003. Available at http://www.globalsecurity.org/military/library/report/gao/d03520.pdf (August 2005).

[33] Thom Shanker, *New York Times*, "U.S. Pushes to Rely More on Remotely Piloted Craft," 5 June 2008. Available at http://www.nytimes.com/2008/06/05/washington/05military.html?_r=1 (September 2005).

[34] Kenneth Corso, Raymond Lewis, Mark Vandroff, and Rich Wiersteiner., *Automated Common Diagrams*, presented at the American Society of Naval Engineers Reconfiguration and Survivability Symposium, Atlantic Beach, FL, February 17, 2005. Available at http://www.caps.fsu.edu/ASNE_Conference/Thur_Presentations/Thur_4/Shipboard_Applications/Corso.pdf (June 2005).

[35] Carderock Division NAVSEA website: http://www.dt.navy.mil/mac-res-eng/mac-inf-sen/mac-con-sys/sof-dev-tec/pro/ (September 2008).

[36] Naval Sea Systems Command, United States Navy, *Integrated Assessment System: CDS Developer Manual*.

[37] Naval Sea Systems Command, United States Navy, *Integrated Assessment System: Operator/Supervisor User Manual*.

[38] Website: "CERT Statistics, 1988-2008." Available at http://www.cert.org/stats/fullstats.html#historic (August 2008).

[39] Computer Security Institute, "2007 CSI Computer Crime and Security Survey," by Robert Richardson, 2007. Available at http://www.gocsi.com (August 2008).

[40] Congressional Research Service, CRS Report for Congress RL32114, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, by Clay Wilson, Library of Congress, 17 October 2003. Available at http://www.fas.org/irp/crs/RL32114.pdf (August 2005).

[41] Computer Emergency Response Team (CERT) Coordination Center, *Overview of Attack Trends*, Carnegie Melon University, 2002. Available at http://www.cert.org/archive/pdf/attack_trends.pdf (August 2005).

[42] Congressional Research Service, CRS Report for Congress RL31534. *Critical Infrastructures: Control Systems and the Terrorist Threat*, by Dana Shea, Library of Congress, 20 January 2004. Available at http://fpc.state.gov/documents/organization/39559.pdf (August 2005).

[43] Website: “Power Peril,” 10 April 2004. Available at http://globalguerrillas.typepad.com/globalguerrillas/2004/04/power.html (August 2005).

[44] Sandia National Laboratories, *Common Vulnerabilities in Critical Infrastructure Control Systems*, by Jason Stamp, John Dillinger, and William Young, 22 May 2003. Available at www.sandia.gov/scada/documents/031172C.pdf (August 2005).

[45] Sandia National Laboratories, *Sandia SCADA Program High Security SCADA LDRD Final Report*, by Rolf Carlson, April 2002. Available at www.sandia.gov/scada/documents/020729.pdf (August 2005).

[46] University of North Carolina Charlotte, *sSCADA: Securing SCADA Infrastructure Communications*, by Yongge Wang and Bei-Tseng Chu,, 05 August, 2004. Available at eprint.iacr.org/2004/265.pdf (August 2005).

[47] Bill Gertz, “Computer Hackers Could Disable Military; System Compromised in Secret Exercise,” *Washington Times*, 16 April 1998. Available at http://lists.jammed.com/ISN/1998/04/0015.html (August 2005).

[48] Gregory Slabodkin, “Calibration Flaw Crashed Yorktown LAN,” *Government Computer News*, Volume 17, Number 30, 09 November 1998. Available at http://www.gcn.com/17_30/news/33914-1.html. (August 2005).

[49] Barton Gellman, “Cyber Attacks by Al Qaeda Feared,” *Washington Post*, 27 June 2002. Available at http://cartome.org/aq-cyberattacks.htm (August 2005).

[50] National Transportation Safety Board, Safety Recommendation, 11 October 2002. Available at http://www.ntsb.gov/Recs/letters/2002/P02_04_05.pdf (August 2005).

[51] Kevin Poulson, “Slammer Worm Crashed Ohio Nuke Plant,” *Security Focus*, 19 August 2003. Available at http://www.securityfocus.com/news/6767 (July 2005).

[52] Website: “CIA: Hackers Shut Down Foreign Power Grid,” 23 January 2008. Available at http://www.foxnews.com/story/0,2933,324547,00.html (June 2009).

[53] United States Department of Defense, Department of Defense Instruction Number 8500.2, *Information Assurance Implementation*, February 6, 2003. Available at http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf (August 2008).

[54] United States Department of Defense, Department of Defense Directive Number 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, 30 December 1997. Available at http://www.dtic.mil/whs/directives/corres/text/i520040p.txt (August 2005).

[55] United States Department of Defense, Department of Defense Directive Number 8100.1, *Global Information Grid (GIG) Overarching Policy*, 19 September 2002. Available at www.dtic.mil/whs/directives/corres/pdf/810001p.pdf (August 2008).

[56] Lunarline Inc., "An Introduction to Department of Defense IA Certification and Accreditation Process", by Mike Bendel, March 2006. Available at www.lunarline.com/docs/Lunarline_DIACAP_Process.pdf (September 2008).

[57] United States General Accounting Office, GAO-05-483T, *Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements*, 7 April 2005. Available at http://www.gao.gov/new.items/d05483T.pdf (August 2005).

[58] United States General Accounting Office, GAO-08-496T, *Information Security: Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies*, 14 February 2008. Available at http://www.gao.gov/new.items/d08496t.pdf (August 2008).

[59] United States General Accounting Office, GAO-04-376, *Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation*, June 2004. Available at http://www.gao.gov/new.items/d04376.pdf (August 2005).

[60] United States General Accounting Office, GAO-07-528, *Information Security: Selected Departments Need to Address Challenges in Implementing Statutory Requirements*, 14 February 2008. Available at http://www.gao.gov/new.items/d07528.pdf/d08496t.pdf (August 2008).

[61] United States General Accounting Office, GAO-05-552, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, July 2005. Available at http://www.gao.gov/new.items/d05552.pdf (September 2008).

[62] United States General Accounting Office, GAO-06-527T, *Information Security: Federal Agencies Show Mixed Progress in Implementing Statutory Requirements*, 16 March 2006. Available at http://www.gao.gov/new.items/d06527t.pdf (September 2008).

[63] United States General Accounting Office, GAO-07-351, *Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program*, May 2007. Available at http://www.gao.gov/new.items/d07351.pdf (December 2008).

[64] United States General Accounting Office, GAO-07-837, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, July 2007. Available at http://www.gao.gov/new.items/d07837.pdf (September 2008).

[65] United States General Accounting Office, GAO-06-178, *Electronic Government: Agencies Face Challenges in Implementing New Federal Employee Identification Standard*, February 2006. Available at http://www.gao.gov/new.items/d06178.pdf (December 2008).

[66] United States General Accounting Office, GAO-08-551T, *Employee Security: Implementation of Identification Cards and DOD's Personnel Security Clearance Program Need Improvement*, 9 April 2008. Available at http://www.gao.gov/new.items/d08551t.pdf (December 2008).

[67] United States Department of Commerce, National Institute of Standards and Technology Special Publication 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007. Available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf (June 2009).

[68] United States General Accounting Office, GAO-08-571T, *Information Security: Progress Reported, But Weaknesses at Federal Agencies Persist*, 12 March 2008. Available at http://www.gao.gov/new.items/d08571T.pdf (August 2008).

[69] United States General Accounting Office, GAO-07-65, *Information Security: Agencies Need to Develop and Implement Adequate Policies for Periodic Testing*, October 2006. Available at http://www.gao.gov/new.items/d0765.pdf (August 2008).

[70] United States General Accounting Office, GAO-07-310, *High-Risk Series: An Update*, January 2007. Available at http://www.gao.gov/new.items/d07310.pdf (November 2008).

[71] United States General Accounting Office, GAO-05-388, *Information Security: Federal Agencies Need to Improve Controls Over Wireless Networks*, May 2005. Available at http://www.gao.gov/new.items/d05388.pdf (November 2008).

[72] United States General Accounting Office, GAO-08-525, *Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains*, June, 2008. Available at http://www.gao.gov/new.items/d08525.pdf (November 2008).

[73] Naval Sea Systems Command, United States Navy, *Integrated Assessment System: System Administrator Manual*

[74] Space and Warfare Systems Center San Diego, *System Security Authorization Agreement (SSAA) for the CVN-93 NIMITZ CLASS Smart Carrier Hull Mechanical & Electrical (HM&E) System*, June 2005.

[75] Michael DiUlio, Chris Savage, Brian Finley, and Eric Schneider, *Taking the Integrated Condition Assessment System To The Year 2010*, presented at the Thirteenth International Ship Control Systems Symposium (SCSS) in Orlando, Florida, April, 2003.

[76] "Remote Monitoring - SWE Improves Equipment Operating Condition Feedback To Support Fleet Readiness," *CHIPS Magazine*, July 2008. Available at http://www.chips.navy.mil/archives/08_jul/web_pages/index.html. (September 2008).

[77] Keith E. Doyne and Daniel E.Martinez, "NAVSEA's HM&E Equipment Data Research System —HEDRS," *Navy Supply Corps Newsletter*, Sept-Oct, 2003. Available at http://findarticles.com/p/articles/mi_m0NQS/is_5_66/ai_107836613/pg_1?tag=artBody;col1 (September 2008).

[78] Paul Oman, Axel Krings, Daniel DeLeon, and Jim Foss, "Analyzing the Security and Survivability of Real-Time Control Systems," *Proceedings of the IEEE Information Assurance Workshop, 2004*. 10-11 June 2004.

[79 The Common Criteria for Evaluation and Validation Scheme website: http://www.niap-ccevs.org/cc-scheme/eval-primer.cfm (August 2008).

[80] Common Criteria for Information Technology Security Evaluation, Part 1. Version 3.0, Revision 2, June 2005. Available at http://www.commoncriteriaportal.org/files/ccfiles/CCMB-2005-07-001.pdf (August 2005).

[81] Sandia National Laboratories, Sandia Report SAND2000-0922, *A Protection Profile for TASE.2*, May 2000. Available at http://www.osti.gov/bridge/servlets/purl/756047-mjBOdK/webviewable/756047.PDF (August 2005).

[82] Decisive Analytics, *System Protection Profile-Industrial Control Systems, Version 1.0* , by Ron Elton, Terry Fletcher, and Matt Earley, June 2004. Available at http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.pdf (August 2005).

[83] Decisive Analytics, *System Protection Profile-Critical Infrastructure Industrial Control Systems, Version 1.07*, by Lynne Ambuel, Ron Melton, Terry Fletcher, and Matt Earley, June 2005.

[84] Digital Bond, *Control Center Protection Profile for Industrial Control Systems, Version .50 (Draft)*, by Dale Peterson, 17 February 2004. Available at http://www.digitalbond.com/SCADA_security/PP_05.pdf (August 2005).

[85] William Jackson, "Under Attack," *Government Computer News*, 13 August 2007. Available at http://www.gcn.com/print/26_21/44857-1.html?page=4 (September 2008).

[86] North American Electric Reliability Council, *Security Guidelines for the Electricity Sector*, Version 1.0, 14 June 2002. Available at http://www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricitySector-Version1.pdf (September, 2005).

[88] Idaho National Engineering and Environmental Laboratory, INEEL/EXT-04-02462, *A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment*, 5 November 2004. Available at http://igs.nigc.ir/IGS/STANDARD/AGA/OIL-GAS-stands.pdf (September 2005).

[89] Chemical Industry Data Exchange, *Guidance for Addressing Cybersecurity in the Chemical Sector*, Version 2.1, May 2005. Available at https://www.pcsforum.org /events/2005/spring/documents/CIDX%20Cybersecurity%20Initiatives_Heard.pdf (September 2005).

[90] United States Department of Energy, *21 Steps to Improve Cyber Security of SCADA Networks*. Available at http://www.oe.netl.doe.gov/docs/prepare /21stepsbooklet.pdf (September 2005).

[91] Idaho National Laboratory, INL/EXT-06-11516, *Revision 3, Cyber Security Procurement Language for Control Systems, Version 1.8*, February 2008. Available at http://www.msisac.org/scada/documents/4march08scadaprocure.pdf (June 2009).

[92] British Columbia Institute of Technology, National Infrastructure Security Coordination Center, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, Version 1.4, 14 February 2005. Available at www.uniras.gov.uk/niscc/scada-en.pdf (September 2005).

[93] Dale Peterson, "Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks," *Intech*, May 2004. Available at http://www.digitalbond.com/SCADA_security/ISA%20Automation%20West.pdf (August 2004).

[94] Andrew K. Wright, John A. Kinast, and Joe McCarthy, "Low-Latency Cryptographic Protection for SCADA Communications," 2004. Available at scadasafe.sourceforge.net/security.pdf (July 2005).

[95] American Gas Association, AGA Report 12, *Cryptographic Protection of SCADA Communications, Part1: Background, Policies, and Test Plan*, Draft 4, 1 November 2004. Available at http://www.awwarf.org/research/TopicsAndProjects/Resources/SpecialReports/2969/AGAPart1.pdf (September 2005).

[96] Rysavy White Paper, “Secure Wireless Networking Using SSL VPNs,” by Peter Rysavy. Available at http://www.aventail.com/downloads/pdfs/WLAN_WP.pdf (3 September 2005).

[97] Sandia National Laboratories, *Framework for SCADA Security Policy*, by Dominique Kilman and Jason Stamp, 2005. Available at www.sandia.gov/scada/documents/sand_2005_1002C.pdf (July 2005).

[98] PC Tools website: http://www.pctools.com/guides/security/id/21/ (January 2009).

[99] United States Department of Defense, Department of Defense Directive Number 8500.1, *Information Assurance*, 24 October 2002. Available at www.acq.osd.mil/ie/bei/pm/ref-library/dodd/d85001p.pdf (August 2008).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California